



Calhoun: The NPS Institutional Archive
DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2019-06

COMBATING STRATEGIC WEAPONS OF INFLUENCE ON SOCIAL MEDIA

Walker, Robert E.

Monterey, CA; Naval Postgraduate School

<http://hdl.handle.net/10945/62826>

Downloaded from NPS Archive: Calhoun



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**COMBATING STRATEGIC WEAPONS OF INFLUENCE
ON SOCIAL MEDIA**

by

Robert Walker

June 2019

Co-Advisors:

James J. Wirtz
Scott E. Jasper

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2019	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE COMBATING STRATEGIC WEAPONS OF INFLUENCE ON SOCIAL MEDIA			5. FUNDING NUMBERS	
6. AUTHOR(S) Rober Walker				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) This thesis provides an overview of how the Russian Federation deploys strategic weapons of influence through social media with the intent to weaken the United States. The thesis asserts that these influence weapons are a direct threat to U.S. national security and have not been completely neutralized by present countermeasures. In an effort to improve the U.S. response to this threat, this thesis seeks to answer the following questions: (1) How effective has the U.S. government's response been to countering Russia's strategic weapons of influence on social media from the 2016 U.S. presidential election through the end of 2018? (2) How effective has the social media industry's self-regulation been in preventing further platform exploitation by strategic weapons of influence during the same time frame? It finds that both the present governmental and private sector responses have not completely blunted this threat. The Kremlin's continued propagation of socially corrosive, divisive narratives over social media highlights the need for an improved response capability that includes cognitive defenses and a government-housed alert mechanism.				
14. SUBJECT TERMS propaganda, social media, information warfare, active measures, influence operations, democracy, social discourse, hybrid warfare, bots, trolls, cyber, psychological operations, Soviet Union, Russia, Facebook, Twitter, Instagram, Google, big data, data analytics, micro targeting, 2016 presidential election			15. NUMBER OF PAGES 147	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

COMBATING STRATEGIC WEAPONS OF INFLUENCE ON SOCIAL MEDIA

Robert Walker
Resident Agent in Charge, Wilmington Resident Office, United States Secret Service,
Department of Homeland Security
BA, George Mason University, 1992

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
June 2019**

Approved by: James J. Wirtz
Co-Advisor

Scott E. Jasper
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis provides an overview of how the Russian Federation deploys strategic weapons of influence through social media with the intent to weaken the United States. The thesis asserts that these influence weapons are a direct threat to U.S. national security and have not been completely neutralized by present countermeasures. In an effort to improve the U.S. response to this threat, this thesis seeks to answer the following questions:

(1) How effective has the U.S. government's response been to countering Russia's strategic weapons of influence on social media from the 2016 U.S. presidential election through the end of 2018?

(2) How effective has the social media industry's self-regulation been in preventing further platform exploitation by strategic weapons of influence during the same time frame?

It finds that both the present governmental and private sector responses have not completely blunted this threat. The Kremlin's continued propagation of socially corrosive, divisive narratives over social media highlights the need for an improved response capability that includes cognitive defenses and a government-housed alert mechanism.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	AN ASSAULT ON FREE MINDS: RUSSIA’S STRATEGIC WEAPONS OF INFLUENCE	1
A.	PROBLEM STATEMENT—THE AMERICAN DEMOCRACY ATTACKED	4
B.	RESEARCH QUESTION	5
C.	RESEARCH DESIGN	6
II.	LITERATURE REVIEW WITH HISTORICAL PERSPECTIVE	9
A.	SOVIET AND RUSSIAN DOCTRINE AND TACTICS	10
B.	THE 2016 U.S. PRESIDENTIAL ELECTION AND ONGOING RUSSIAN STRATEGY	35
C.	COMBATING INFLUENCE OPERATIONS/STRENGTHENING DEMOCRACY	45
D.	TRACKING THE BOTS AND TROLLS	47
E.	THE PRESENT RESPONSE, GOVERNMENTAL, AND CORPORATE	66
F.	CONCLUSIONS FROM LITERATURE	68
III.	THE KREMLIN’S SOCIAL MEDIA ATTACK ON THE 2016 U.S. PRESIDENTIAL ELECTION—A DIAGNOSIS	69
A.	LAYERS OF DECEPTION	69
B.	ATTACKS ON REASON	71
C.	INFORMATION WEAPON DEPLOYMENT	72
D.	TARGETING VULNERABILITIES WITH AMPLIFIED AUTHENTIC CONTENT	76
E.	A CONCLUSION: WELL-REASONED DECEPTION THROUGH AMPLIFIED NARRATIVES	79
IV.	THE RESPONSE TO THE KREMLIN ATTACK	81
A.	THE U.S. GOVERNMENT: PROTEST, PUNISHMENT, AND CONGRESS LEARNS THAT SOCIAL MEDIA COMPANIES SELL ADVERTISING	81
B.	TWO-FACEBOOK	84
C.	TWITTER	86
D.	INVESTIGATIONS LAUNCHED, CRIMINALS CHARGED, REGULATIONS PROPOSED, AND TECH GIANTS ADAPT	86
V.	IMPACT OF RESPONSE	89

A.	THE KREMLIN’S PERSISTENCE	89
B.	JUSTICE FINDS EVIDENCE, “PROJECT LAKHTA”	90
C.	TORMENT THE TORMENTOR.....	93
D.	DIGITAL FORENSIC LAB OBSERVATIONS/ MEDIUM AND HAMILTON 68.....	94
VI.	OBSERVATION AND RECOMMENDATIONS FOR FUTURE POLICIES: TRANSPARENCY, EDUCATION, AND AWARENESS	101
A.	COMBATING STRATEGIC WEAPONS OF INFLUENCE WILL REQUIRE POLITICAL UNITY AND PUBLIC AWARENESS	101
B.	RAISE THE COST, AND FOLLOW OUR OWN ADVICE.....	101
C.	BUILD ON THE PRESENT	103
D.	ENGAGING THE WHOLE SOCIETY	106
E.	NO TIME FOR COMPLACENCE.....	111
	LIST OF REFERENCES	113
	INITIAL DISTRIBUTION LIST	123

LIST OF FIGURES

Figure 1.	Content from the Russian Social Media Account “Afro Kingdom.”	12
Figure 2.	Content from the Russian Instagram Account “Black Matters.”	13
Figure 3.	Content from the Russian Social Media Account “Being Patriotic.”	14
Figure 4.	Content from the Russian Social Media Account “USA Gunslinger.”	15
Figure 5.	Content from the Russian Social Media Account “Angry Eagle.”	16
Figure 6.	Content from the Russian Social Media Account “Woke Blacks.”	17
Figure 7.	Content from the Russian Social Media Site “Jenna Abrams.”	19
Figure 8.	Content from the Russian Social Media Site “Jenna Abrams.”	20
Figure 9.	Content from the Russian Social Media Site “Jenna Abrams.”	21
Figure 10.	Content from the Russian Social Media Site “Jenna Abrams.”	22
Figure 11.	Content from the Russian Social Media Site “Jenna Abrams.”	23
Figure 12.	Content from the Russian Social Media Site “Jenna Abrams.”	24
Figure 13.	Content from the Russian Social Media Account “PamelaMoore13.”	25
Figure 14.	Content from the Russian Social Media Account “Pamela Moore13.”	26
Figure 15.	Content from the Russian Social Media Account “Pamela Moore13.”	27
Figure 16.	Content from the Russian Social Media Account “Pamela Moore13.”	28
Figure 17.	Content from the Russian Social Media Account “Pamela Moore13.”	29
Figure 18.	Content from the Russian Social Media Account “Pamela Moore13.”	30
Figure 19.	Content from the Russian Social Media Account “Pamela Moore13.”	31
Figure 20.	A Comparative Timeline of the Spread of Anti-American Rumors before and after the Advent of Social Media, as It Appeared on the Website Hamilton 68.	33
Figure 21.	Normalization of Political Views with Facebook Abstinence, as Published by Stanford University.	35

Figure 22.	Content from the Russian Social Media Account “AmericaFirst.”	37
Figure 23.	Content from the Russian Social Media Account “Anonymous News.”	38
Figure 24.	Content from the Russian Twitter Account “Jenna Abrams.”	39
Figure 25.	Content Refencing Deceased U.S. Navy Seal Christopher Kyle, from the Russian Social Media Account “Veterans US.”	40
Figure 26.	Content from the Russian Twitter Account “Jenna Abrams.”	41
Figure 27.	Content from the Russian Social Media Account “Pamela Moore13.”	42
Figure 28.	Content from the Russian Twitter Account “TEN GOP.”	44
Figure 29.	Content from the Russian Instagram Account “Black Matters.”	49
Figure 30.	Content from the Russian Social Media Account “USA Gunslinger.”	50
Figure 31.	Content from the Russian Social Media Account “South United.”	51
Figure 32.	Content from the Russian Social Media Account “Woke Blacks.”	52
Figure 33.	Content from the Russian Social Media Account “Secure Borders.”	53
Figure 35.	Content from the Russian Social Media Account “Army of Jesus.”	55
Figure 36.	Content from the Russian Social Media Account Stop All Invaders.”	56
Figure 37.	Content from the Russian Social Media Accounts “Merican Fury.”	57
Figure 38.	Content from the Russian Social Media Account “Stop All Invaders.”	58
Figure 39.	Content from the Russian Twitter Account “Jenna Abrams.”	59
Figure 40.	Content from the Russian Social Media Account “Born Liberal.”	60
Figure 41.	Content from the Russian Social Media Account “Muslim Voice.”	61
Figure 42.	Content from the Russian Social Media Account “Rainbow Nation US.”	62
Figure 43.	Content from the Russian Social Media Account “Army of Jesus.”	63
Figure 44.	Content from the Russian Social Media Account “Feminism Tag.”	64

Figure 45.	Content from the Russian Social Media Account “Merican Fury.”	65
Figure 46.	Types of Misinformation/Disinformation as Listed in Harvard’s <i>First Draft</i>	70
Figure 47.	Graphic Displaying Logical Fallacies from the Digital Forensic Research Lab.....	71
Figure 48.	Associated Press Chart of Russian Twitter Traffic.....	73
Figure 49.	Content from the Russian Twitter Account “TEN GOP.”	75
Figure 50.	Berkman-Klein Chart of Media Sources Amplified by Russia’s Propagandists.	77
Figure 51.	Berkman-Klein Chart of Russian Troll Twitter Account Activity.	78
Figure 52.	Internet Research Agency Twitter Activity as Compiled by the Computational Propaganda Project.....	90
Figure 53.	Content from the Russian Social Media Account “AmericaFirst.”	94
Figure 54.	Digital Forensic Research Lab Compilation of Grammatical Errors in Russian Content.	96
Figure 55.	Digital Forensic Research Lab Image Showing Watermarks in Two Generations of Russian Content.....	97
Figure 56.	Digital Forensic Research Lab Image Sputnik Sourced Language on Fallacious Instagram Post.	98
Figure 57.	Content from the Russian Social Media Account “Angry Eagle.”	100
Figure 58.	Sign Posted Out Front of the Alvarado Street Brewery, Monterey CA, 2018. Attribution to Abraham Lincoln Has Not Been Verified.	112

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY OF TERMS

Astroturfing—Refers to creating buzz around a subject by posting what appear to be multiple spontaneous, anonymous comments, be they to social media, a blog, a webpage comments section, or wiki, etc. The posts, while appearing random and uncoordinated, are in fact orchestrated for effect by a propagandist, which may be a public relations firm but can also be a governmental entity. This term alludes to the ubiquitous artificial grass designed to look real, as used on many sports playing fields and lawns in drought-plagued areas. It can also be found at the base of the flagpole in front of Herrmann Hall at the Naval Postgraduate School, Monterey, CA.

Botnet—Refers to a legion of compromised or virus infected computers used to spread nefarious content, viruses, overload servers, and perform other illegitimate automated tasks.

Bot—Refers to an automated program tasked to execute a repetitive function on the internet. In the context of propaganda, a bot could be used to post content that appears to be organically created by an authentic human account that thus furthers an astroturfing campaign. Bots can also be used to search the internet for certain terms or types of content to either amplify or nullify that content.

Clickbait—Refers to a misleading or inaccurate headline-styled post that lures those who view it to click on the site. Often times, the provocative nature of the clickbait headline is more sensational than the content to which it directs the user. Clickbait is used by both commercial and political propagandists.

Gaslighting—Refers to a psychological manipulation technique akin to brainwashing that is deployed to gain power over a targeted individual or group by distorting the targets' reality. It is done slowly over time to keep the victims unaware of the process to convince the targets that false information is factual, which then slowly erodes the targets' grip on reality and thus builds reliance on the purveyors of the false information.

Sock puppet—Refers to aliases or fake persona created by social media users to masquerade as someone or something else on the internet. The false nature of the sock puppet allows them to make controversial or offensive comments while taking sides on a particular issue without the risk of exposing their real identity. Sock puppets have been known to post commentary on content that they might have produced themselves under a different identity.

Troll—Refers to a person or persons who post inflammatory often false social media content or remarks to provoke a desired reaction, engage in harassment, or generate negative discourse. Trolls often conceal their real identity or post anonymously and thus assume little risk for making inflammatory remarks compared to making them openly or in person.

Watermark (Digital)—Refers to a data pattern secreted into a digital file that, while not easily detected by a casual internet user, can identify a piece of content's origin or authenticity. While digital watermarks are often inserted to deter the illegal distribution of commercial content and intellectual property, they can also be used to track nefarious content.

LIST OF ACRONYMS AND ABBREVIATIONS

AP	Associated Press
CSIS	Center for Strategic and International Studies
DHS	Department of Homeland Security
DNI	Director of National Intelligence
JAR	Joint Activity Report
MIT	Massachusetts Institute of Technology
MSB	Swedish Civil Contingencies Agency
MSM	mainstream media
NGO	non-governmental organization

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

In 2016, the Russian Federation mounted a large-scale active-measures campaign targeting the U.S. presidential election.¹ The full extent of this strategic weapon of influence is still being investigated for both its impact on the electoral process and its greater effect on national discourse. During the run up to the election, the Kremlin's attack enhanced existing social and political divides by using false information and emotionally provocative narratives in part spread through social media.² While the psychology of this type of attack was not new, the Kremlin's strategists exploited a modern media environment that now includes internet-based social media in addition to traditional journalism (print, radio, television) to disseminate their hostile messages to target audiences. While much public debate has been focused on this attack's impact on a presidential election, its overall goal was to diminish the effectiveness of American political institutions and the quality of the policy-making process in the United States.

This attack was documented in the Joint Activity Report (JAR) produced by the Department of Homeland Security (DHS) in December 2016 and the assessment by the Director of National Intelligence (DNI) from January 2017.³ The report chronicled the use of both mainstream media and social media to spread divisive propaganda. It further noted that Vladimir Putin's objective in ordering this active measures campaign was to undermine the confidence Americans have in their democratic processes.⁴ Defining the

¹ Senate Select Committee on Intelligence, *The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections* (Washington, DC: Senate Select Committee on Intelligence, 2018), 1–7, https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf.

² Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution* (Washington, DC: National Intelligence Council, 2017), 1–14, https://permanent.access.gpo.gov/gpo76345/ICA_2017_01.pdf.

³ National Cybersecurity and Communications Integration Center, *Grizzly Steppe Russian Malicious Cyber Activity*, JAR-16-20296 (Washington, DC: Department of Homeland Security/Federal Bureau of Investigation, 2016), 1–13, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf; Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections,"* 1–14.

⁴ Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, 3–6.

aims of this type of influence operation highlights the potential danger it poses to the American people.

A 2011 Russian Federation Armed Forces document provided the following definition for information warfare:

Information War is the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force.⁵

It is through this lens of information warfare that the 2016 Kremlin interference in the U.S. election is considered in this thesis. It also provides a perspective into Moscow's efforts preceding the 2018 U.S. midterm elections, as it continued its attempted assault on American civil society using social media platforms.

To assist the reader with understanding this threat, this document provides a broader look at influence operations or active measures within its literature review, in particular as they have been implemented by the Soviet Union or Russia. It provides a historical perspective on where these strategic weapons of influence fit into a broader information warfare strategy, while it examines the overall psychological foundations for how they function when deployed.

Contained throughout this thesis are actual examples of social media content either created, disseminated, or amplified by Russia, and in particular, propaganda linked to the Internet Research Agency in Saint Petersburg. These examples were chosen to display the diverse, divisive, and socially corrosive nature of the propaganda. This material is emotionally evocative, and often offensive, and is designed to push the reader or viewer's minds outside a rational framework. If those reading this thesis find themselves angry, sad, empathetic, or supportive of one cause or another, they are

⁵ Ministry of Defence of the Russian Federation, *Russian Federation Armed Forces' Information Space Activities Concept* (Moscow: Ministry of Defence of the Russian Federation, 2011), <https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle>.

experiencing the force of this political instrument. Emotional reaction shows the power of these strategic weapons of influence and why the Kremlin uses them.

Underlying the research is the hypothesis that U.S. countermeasures implemented through 2018 have only been partially effective in combating social media exploitation by Russia's strategic weapons of influence. This thesis asserts that both the present U.S. governmental and private sector responses have not completely blunted or deterred this threat. While the government as well as social media companies have made strides towards cooperating in combating this problem, particularly in the areas of identification and neutralization of hostile content, more needs to be done. The thesis acknowledges that the solutions for combating this threat in 2019, be they governmental or industry-based, will likely not evolve as fast as the technology or tactics used to launch future assaults. Thus, this thesis identifies additional strategies for reducing the impact of this type of attack on American social and political discourse.

This thesis in order to identify additional counter strategies, also assesses the efficacy of the present responses to these ongoing attacks against the U.S. democracy. To do so, it seeks to answer the following questions: (1) How effective has the U.S. government's response been to countering strategic weapons of influence deployed by Russia over social media from the 2016 U.S. presidential election through the end of 2018? and (2) How effective has the social media industry's self-regulation been in preventing further platform exploitation by strategic weapons of influence during the same time frame?

Some solutions proposed in this thesis come from psychological research while others come from the experience of the Nordic nations that have been targeted by Russian active measures since the emergence of the tactic in the Soviet era. The Kremlin's continued propagation of socially corrosive, divisive narratives over the internet are used to highlight the need for an improved response capability, which includes engaging the whole of society, building cognitive defenses, and using a government housed alert mechanism to heighten the American people's awareness of the threat.

The thesis asserts that policy makers should not assume what works today for monitoring and mitigation of social media-based influence operations will work tomorrow. The strategy to countering strategic weapons of influence must be comprehensive and adaptable. It should include elements of today's response like diplomatic sanctions, economic sanctions, criminal prosecution, private sector self-regulation, as well as the ongoing efforts of non-governmental organizations and the free press to track the threat. Nevertheless, this thesis identifies additional elements not yet present in the U.S. counter strategy that should be added. Elements include engaging all sectors of civil society, as well as government supported educational programs that prepare Americans for future attacks. In addition to propaganda education, the government should openly provide alerts when a largescale attack is identified. To simply fall back on the private sector regulation and non-governmental monitoring is not enough. A Department of Homeland Security warning system can provide credibility to the threat, while potentially increasing faith in government institutions and the democratic processes that supports them.

These counter strategies are proposed with an understanding for the likely malleability of delivery medium for future active measures campaigns. They transcend rapidly evolving technology and inevitable changes in the media environment. They offer an opportunity not just to blunt the impact of present strategic weapons of influence, but also to strengthen fundamentally the integrity of the U.S. democracy, on which this nation's economic vibrancy and global leadership are built.

ACKNOWLEDGMENTS

There are no words sufficient to describe my gratitude for the support I have received during this journey. Without the love of my family, understanding of my friends, and encouragement of my peers, this project would not have been.

To my family, you reminded me every day why this work is important while holding me together through months of research, reading, and writing. To my better half, without complaint, you set aside so much so I could achieve this goal. I could not have done this without you. To my oldest, you are an absolute inspiration. Your dedication to excellence and academic brilliance set the bar very high indeed. To my youngest, your quiet success and love for life provided me with great perspective. To the matriarch, your barrier smashing, dedicated, courageous professionalism never escaped me growing up, nor these past months.

To the faculty and staff of the Center for Homeland Defense and Security and your compatriots at the Naval Postgraduate School, you are as talented as you are dedicated. Thank you for striving to make the nation safer and for including me in this quest. To Dr. Cris Matei, the encouragement you gave me for this work speaks to your concern for our democracy. Keep spreading the word, we need you! To Dr. Chris Bellavita, your search for truth, balance, and excellence pervade this program; however, your sincere interest in our success is your most commendable trait. May the force be with you!

That I would do this project all over again is a reflection on the talent of my advisors. Dr. James Wirtz, you are a true professional and a master of your craft. You drove me forward when I needed driving and let me breathe when I needed to breathe. Dr. Scott Jasper, from our first conversations, you believed in this work. Your succinct recommendations for both the subject, as well as the process, kept me and this project on the rails. Gentlemen, a simple thank you is not enough.

To my classmates, you are an incredible, diverse, and dedicated group, and the nation is lucky to have you at its service. The greatest value I take from this program, and what made this the most extraordinary of experiences, was you. Full stop!

To my friends in Delaware, the kindness you showed me this past year permitted me to stand when I could have fallen and contributed in no small degree to the completion of this work. Your patriotism, wisdom, and optimism for America's future was infectious. I hope that many more can catch your disease.

To my brothers and sisters in the U.S. Secret Service. I have always felt this agency was one big family, never more than during my studies. From my superiors who supported this opportunity to my peers who never failed to provide encouragement, you are all truly Worthy of Trust and Confidence.

I. AN ASSAULT ON FREE MINDS: RUSSIA'S STRATEGIC WEAPONS OF INFLUENCE

More than two years after the Russian social media-based attack on the 2016 U.S. presidential election, Dan Coats, President Donald Trump's appointed Director of National Intelligence (DNI) made the following statement. The date was January 29, 2019. The event was Director Coat's presentation of the intelligence community's 2019 Annual Threat Assessment:

Even as Russia faces a weakening economy, the Kremlin is stepping up its campaign to divide Western political and security institutions and undermine the post-WWII international order. We expect Russia will continue to wage its information war against democracies and to use social media to attempt to divide our societies.¹

DNI Coats, with his statement about Russia's ongoing information warfare *modus operandi*, underlines the problem addressed by this thesis.

This document provides an overview of how the Russian Federation deploys strategic weapons of influence through social media with the intent to weaken the United States. These influence weapons, known to the Kremlin as active measures, or in the liberal democracies as influence operations, are part of an information warfare toolbox. They are deployed against the United States with the goals of weakening America's social fabric, democratic structures, world standing, and its relationship with allied nations.² They present a direct threat to U.S. national security and should be understood as a danger, not a nuisance.

¹ Office of Strategic Communications, *Remarks as Prepared for Delivery by The Honorable Dan Coats, Director of National Intelligence Annual Threat Assessment Opening Statement, Tuesday, January 29, 2019* (Washington, DC: Office of the Director of National Intelligence, 2019), 7, https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-01-29-ATA-Opening-Statement_Final.pdf.

² Senate Select Committee on Intelligence, *The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections* (Washington, DC: Senate Select Committee on Intelligence, 2018), 2–3, https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf.

A 2011 Russian Federation Armed Forces document, translated by the Linguistic Centre of the Russian Federation Defence Ministry, provided the following definition for information warfare:

Information War is the confrontation between two or more states in the information space with the purpose of inflicting damage to information systems, processes and resources, critical and other structures, undermining the political, economic and social systems, a massive psychological manipulation of the population to destabilize the state and society, as well as coercion of the state to take decisions for the benefit of the opposing force.³

It is through this lens of information warfare that the 2016 Kremlin interference in the U.S. election is best considered. It also provides a perspective into Moscow's efforts preceding the 2018 U.S. midterm elections, as it continued its attempted assault on American civil society using social media platforms.

This thesis assesses the efficacy of the present responses to these ongoing attacks against the U.S. democracy. To do so, it seeks to answer the following questions: (1) How effective has the U.S. government's response been to countering strategic weapons of influence deployed by Russia over social media from the 2016 U.S. presidential election through the end of 2018? and (2) How effective has the social media industry's self-regulation been in preventing further platform exploitation by strategic weapons of influence during the same time frame?

Before answering the aforementioned questions, this thesis first describes the 2016 Kremlin directed attack on the U.S. presidential election and how it exploited social media. It identifies the tactics deployed by Russia's propagandists, the audiences they targeted, and their success in leading Americans to act in ways deleterious to civil society.

To illustrate the 2016 attack, the thesis offers a brief history of Russian active measures and information warfare. It illustrates how the Kremlin's information warfare

³ Ministry of Defence of the Russian Federation, *Russian Federation Armed Forces' Information Space Activities Concept* (Moscow: Ministry of Defence of the Russian Federation, 2011), <https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle>.

tacticians have adapted a century-old psychological operations methodology to a modern media environment, where internet-based platforms like Facebook and Twitter, provide billions of users each day with virtually unlimited content.

Contained throughout this thesis are actual examples of social media content either created, disseminated or amplified by Russia, and in particular, propaganda linked to the Internet Research Agency in Saint Petersburg. These examples were chosen to display the diverse, divisive, and socially corrosive nature of the propaganda. This material is emotionally evocative, often offensive, and is designed to push the reader or viewer's minds outside a rational framework. If those reading this thesis find themselves angry, sad, empathetic, or supportive of one cause or another, they are experiencing the force of this political instrument. Emotional reaction shows the power of these strategic weapons of influence and why the Kremlin uses them.

Also examined in this thesis are some of the present responses to the attack on the 2016 election, which include diplomatic protests, expulsions, criminal investigations, economic penalties, proposed legislation and ongoing legal action (any tactical cyber responses from the U.S. government's intelligence and defense agencies are outside the scope of this research). For the social media companies, it explores how they have changed policies, added additional security staff, identified hostile content, and ultimately, removed material indicative of organized propaganda from state level actors.

Additionally, this thesis identifies how nongovernmental organizations and academia have contributed to monitoring and understanding Russia's strategic weapons of influence. The efforts of organizations like the German Marshall Fund and the Atlantic Council to track in real-time online propaganda operations, contributed to this document. Researchers at institutions including, Oxford University, Harvard University, Columbia University, the Massachusetts Institute of Technology, as well as the Naval Postgraduate School, provided a greater understanding of how propaganda travels over the internet, what populations are targeted, and the reach of these influence operations.

This thesis asserts that both the present U.S. governmental and private sector responses have not completely blunted or deterred this threat. While the government and

social media companies have made strides towards cooperating in combating this problem, and in particular, in the areas of identification and neutralization of hostile content, more needs to be done. The thesis acknowledges that the solutions for combating this threat in 2019, be they governmental or industry-based, will likely not evolve as fast as the technology or tactics used to launch future assaults. Some proposed solutions come from psychological research while others come from the experience of the Nordic nations, which have been targeted by Russian active measures since the emergence of the tactic in the Soviet era. The Kremlin's continued propagation of socially corrosive, divisive narratives over the internet are used to highlight the need for an improved response capability, which includes engaging the whole of society, building cognitive defenses, and using a government housed alert mechanism to heighten the American people's awareness of the threat.

A. PROBLEM STATEMENT—THE AMERICAN DEMOCRACY ATTACKED

In 2016, the Russian Federation mounted a large-scale active measures campaign targeting the U.S. presidential election.⁴ The full extent of this strategic weapon of influence is still being investigated for both its impact on the electoral process and its greater effect on national discourse. During the run up to the election, the Kremlin's attack enhanced existing social and political divides by using false information and emotionally provocative narratives in part spread through social media.⁵ While the psychology of this type of attack was not new, the Kremlin's strategists exploited a modern media environment that now includes internet-based social media in addition to traditional journalism (print, radio, television) to disseminate its hostile messages to target audiences. While much public debate has been focused on this attack's impact on a presidential election, its overall goal was to diminish the effectiveness of American political institutions and the quality of the policy-making process in the United States.

⁴ Senate Select Committee on Intelligence, *The Intelligence Community Assessment*, 2–5.

⁵ Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections": The Analytic Process and Cyber Incident Attribution* (Washington, DC: National Intelligence Council, 2017), 2–4, https://permanent.access.gpo.gov/gpo76345/ICA_2017_01.pdf.

This attack was documented in the Joint Activity Report (JAR) produced by the Department of Homeland Security (DHS) in December 2016, and the assessment by the DNI from January 2017.⁶ The report chronicled the use of both mainstream media and social media to spread divisive propaganda. It further noted that Vladimir Putin's objective in ordering this active measures campaign was to undermine the confidence Americans have in their democratic processes.⁷ Defining the aims of this type of influence operation highlights the potential danger it poses to the American people. Underlying this research is the hypothesis that U.S. countermeasures implemented through 2018 have only been partially effective in combating social media exploitation by Russia's strategic weapons of influence.

The targeting of the U.S. elections, political discourse, and legislative processes, took place at a time when public faith in government institutions was already in decline. This reduction of public trust was emphasized in a 2017 Pew research study that documented only 20% of Americans trusted the federal government to do what is right, down from 73% in 1958.⁸ Both the nature of the Kremlin's attack and this preexisting sociopolitical vulnerability provide impetus for this research.

B. RESEARCH QUESTION

This thesis, to identify additional counter strategies, assesses the efficacy of the present responses to ongoing active measures attacks against the U.S. democracy. To do so, it seeks to answer the following questions: (1) How effective has the U.S. government's response been to countering strategic weapons of influence deployed by Russia over social media from the 2016 U.S. presidential election through the end of 2018? and (2) How effective has the social media industry's self-regulation been in

⁶ National Cybersecurity and Communications Integration Center, *Grizzly Steppe Russian Malicious Cyber Activity*, JAR-16-20296 (Washington, DC: Department of Homeland Security/Federal Bureau of Investigation, 2016), 1–13, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf; Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections,"* 1–14.

⁷ Office of the Director of National Intelligence, 1.

⁸ "Public Trust in Government: 1958–2017," Pew Research Center, December 14, 2017, <http://www.people-press.org/2017/05/03/public-trust-in-government-1958-2017/>.

preventing further platform exploitation by strategic weapons of influence during the same time frame?

C. RESEARCH DESIGN

This research evaluates the effectiveness of policies and practices aimed at decreasing the impact of strategic weapons of influence disseminated through social media. Techniques for this study are constrained to those that are in line with contemporary U.S. Constitutional guidelines, in particular interpretations of the First Amendment and that are available for review in the public sphere. It looks at information that shows the effectiveness of government response and private sector self-regulation from the 2016 election through the end of 2018. This research design is broken down into three phases.

Chapter III examines how the Kremlin used social media to disseminate strategic weapons of influence from 2016 through 2018. It evaluates the techniques Russia used to exploit social media from message targeting to message promulgation. The reach and impact of Russia's 2016 attack and ongoing operations are analyzed by reviewing testimony from social media companies, the U.S. Congress, the Executive Branch, academic studies, non-classified intelligence products, court records, think tank research, and contemporary reporting by reputable media outlets.

Chapter IV identifies the public and private sector responses to Russian activities. The context for these responses are those related to limiting the spread of influence related material by nefarious actors through social media and those that better prepare the American people for this type of attack. The scope is to examine responses, be they legislative, legal, diplomatic, regulatory or self-regulatory, that focus on message targeting and message dissemination. Categories include government-imposed remedies and corporate self-regulatory practices. Any tactical cyber responses from the U.S. government's intelligence and defense agencies are outside the scope of this research.

Chapter V identifies relevant documentary evidence of each policy's success or failure. It reviews the policies relevance to the problems identified and the impact on the adversary's tradecraft and the American people's ability to resist it. It examines peer

reviewed policy analysis, contemporary studies, government records, corporate records, non-governmental organizations (NGOs), and think tank reports. One proposed measure of policy performance is to look at automated political influence tracking data currently being produced by NGOs, academic institutions, and where possible (outside a classified environment) from government sources; for example, change (increase or decrease) in active measures bot traffic as related to a government or industry practice aimed at impacting a particular vector.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW WITH HISTORICAL PERSPECTIVE

To understand how the Russian Federation used social media as a delivery mechanism for its contemporary influence operations, it is first necessary to understand better the historical role of strategic weapons of influence in the Kremlin's information warfare arsenal. Historical perspectives were included in this review covering, information warfare, active measures, influence operations, and propaganda. This literature examined encompassed academic studies, governmental records, news media reporting, think tank research, internet sites, as well as non-fiction and fictional literature. As this research involves the Russian active measures campaign targeting the 2016 U.S. presidential election, much of the reviewed literature is contemporaneous to these events, which emphasizes cyber tactics, the internet, and social media.

The Russian government, like its Soviet predecessor, has used active measures as an integral part of its information warfare package. Active measures encompass a list of techniques that formed a Soviet or Russian type of influence operations that became more widely recognized in the 1950s. The term covers overt and covert methods for influencing population behaviors in a targeted state. An active measures campaign could include the undermining of leaders, institutions, disrupting exterior relations, and discrediting opponents both inside and outside of government.⁹ Georgetown University Professor Roy Godson, while defining active measures in testimony to the U.S. Senate in 2017, elaborated that their use often includes deceptive efforts to manipulate both elite members of society, as well as mass audiences in the adversary nation. Godson stated the goal was to, “distort the target’s perception of reality.”¹⁰ This gaslighting may be achieved overtly through officially sponsored media outlets, state propaganda, diplomatic channels, and covertly, through disinformation, agents of influence, clandestine radio, as well as front organizations.¹¹

⁹ Senate Select Committee on Intelligence, *Disinformation a Primer in Russian Active Measures and Influence Campaigns* (Washington, DC: Senate Select Committee on Intelligence, 2017), 10–20, <https://www.gpo.gov/fdsys/pkg/CHRG-115shrg25362/pdf/CHRG-115shrg25362.pdf>.

¹⁰ Senate Select Committee on Intelligence, 20.

¹¹ Senate Select Committee on Intelligence, 10–20.

A. SOVIET AND RUSSIAN DOCTRINE AND TACTICS

The Kremlin's use of active measures as part of its hybrid information warfare package to undermine adversary nations' social discourse has received much academic and governmental attention. Two such papers, one by Jamie Palagi, and another by Christopher S. Chivvis, take an in-depth look at Russian hybrid warfare tactics to include using information as a weapon.¹² While the philosophical illusion of a Marxist-Leninist global revolution no longer exists as a paradigm for the Kremlin's foreign policy, the consensus of much of today's literature is that active measures deployed by Putin's government stem from techniques developed during the Soviet era. A book by Alexander Klimburg, a senior fellow at the Atlantic Council, describes in great detail the Russian view of information as a weapon to be controlled and deployed, along with how this philosophy has been put into practice over the internet. Klimburg's work highlights the link to the Communist past, "From Lenin's very first orders as the ruler of post-revolution Russia to the collapse of the Soviet Union, Communist strategic thinking has revolved around notions of censorship and propaganda, as well as psychological operations and deception."¹³ The Kremlin's deployment of influence weapons against the United States via social media under the orders of President Putin can be tied directly back to Soviet information warfare doctrine.

Little debate arises about the Soviet use of active measures and their extension into the Kremlin's arsenal today. In July 2016, *Business Insider* cited the following quote from retired KGB General Oleg Kalugin, who described Moscow's information and psychological warfare as a way, "to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground

¹² Jamie Palagi, *Wrestling the Bear: The Rise of Russian Hybrid Warfare* (Norfolk, VA: Joint Forces Staff College Joint Advanced Warfighting School, 2015), 23; Christopher S. Chivvis, "Hybrid War: Russian Contemporary Political Warfare," *Bulletin of the Atomic Scientists* 73, no. 5 (August 21, 2017): 316, <https://doi.org/10.1080/00963402.2017.1362903>.

¹³ Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin, 2017), 210.

in case the war really occurs.”¹⁴ Kalugin’s description of the Kremlin’s tactics appears prophetic against the backdrop of current events. The Kremlin’s interference in the 2016 U.S. presidential election, Brexit in the United Kingdom, Catalan Independence in Spain, the rise of nationalist leaders like Marie Le Pen in France, and the public assertion by some U.S. policy makers that the NATO alliance may be obsolete, all reflect developments in line with the Kremlin’s strategic interests.¹⁵

The recent evolution of the Kremlin’s techniques for disinformation requires differentiation beyond the addition of social media exploitation. It has been observed that traditionally effective propaganda requires elements of deception mixed in with a healthy dose of truth and that the messaging should be consistent.¹⁶ The latter part, consistency of message directed at one side of an issue, no longer appears to be a necessary requisite for the Kremlin’s active measures program targeting liberal democracies. In many examples, the Kremlin’s propagandist attacked both sides of issues, provided conflicting messages from one social media post to the next, and quickly adapted new messages to explain contradictions in previous messages.

The Russian disseminated propaganda in Figures 1–6 seeks to provoke emotional responses from different angles concerning race and police shootings in the United States.

¹⁴ Natasha Bertrand, “It Looks like Russia Hired Internet Trolls to Pose as Pro-Trump Americans,” *Business Insider*, July 27, 2016, <http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7>.

¹⁵ “Trump Worries NATO with ‘Obsolete’ Comment,” BBC, January 16, 2017, <https://www.bbc.com/news/world-us-canada-38635181>.

¹⁶ Paul Christopher and Miriam Matthews, *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It* (Santa Monica, CA: RAND, 2016), 1–2, <https://www.rand.org/pubs/perspectives/PE198.html>.



Figure 1. Content from the Russian Social Media Account “Afro Kingdom.”¹⁷

¹⁷ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘AfroKingdom_’,” UsHadrns, October 29, 2017, <https://medium.com/@ushadrns/this-space-is-a-repository-for-content-from-the-russian-twitter-account-afrokingdom-1ec195324086>.

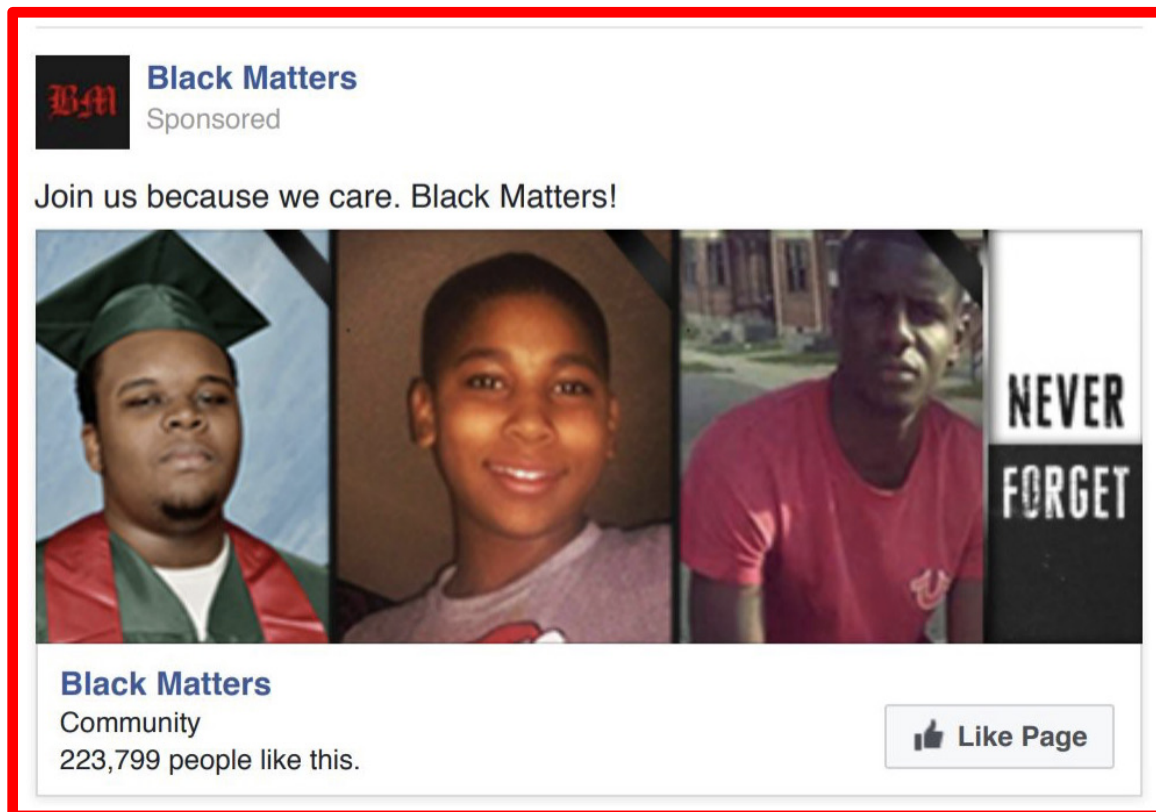


Figure 2. Content from the Russian Instagram Account “Black Matters.”¹⁸

¹⁸ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Watch.the.Police’,” UsHadrons, October 25, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-twitter-account-watch-the-police-e894e0269670>.



Figure 3. Content from the Russian Social Media Account “Being Patriotic.”¹⁹

¹⁹ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Being Patriotic’,” UsHadrns, October 12, 2017, <https://medium.com/@ushadrns/this-space-is-a-repository-for-ads-from-the-russian-social-media-group-being-patriotic-4e823cad0a02>.



Figure 4. Content from the Russian Social Media Account “USA Gunslinger.”²⁰

The Russian disseminated propaganda in Figures 5 and 6, take on different sides of the issues surrounding race, patriotism, and the National Anthem in the regards to the protest by NFL quarterback Colin Kaepernick.

²⁰ Source: “This Space Is a Repository for Content from the Russian Twitter Account ‘USA_Gunslinger’,” UsHadrons, October 30, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-twitter-account-usa-gunslinger-538485a9224f>.

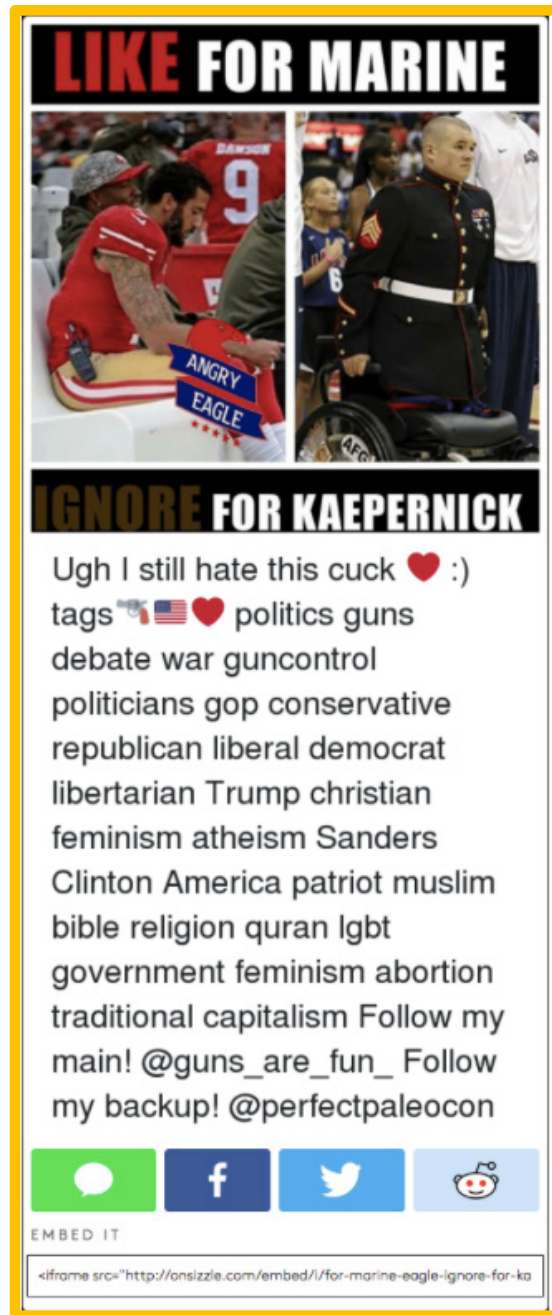


Figure 5. Content from the Russian Social Media Account “Angry Eagle.”²¹

²¹ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Angry Eagle,’” UsHadrns, October 18, 2017, <https://medium.com/@ushadrns/this-space-is-a-repository-for-content-from-the-russian-social-media-group-angry-eagle-84d85140e71>.

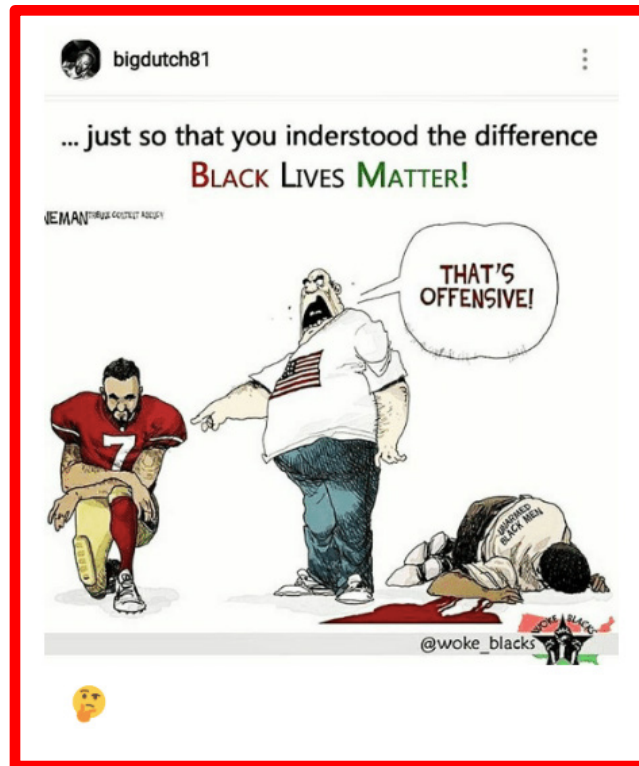


Figure 6. Content from the Russian Social Media Account “Woke Blacks.”²²

An overriding purpose to this inconsistent messaging is to create confusion, and thus, make it difficult for the targeted populations to distinguish truth from fiction. This messaging allows the imbedding of themes that interest Russia’s overall objectives once the source has been accepted as credible by the target. In other words, since individuals no longer know what to believe, they will trust what they are told because of affection or perceived credibility.²³ Many of the sites created by the Russian Internet Research Agency did not immediately start disseminating information to support a particular strategic purpose, but spent months building a loyal list of followers before weaponizing its messaging. These tactics were documented in 2015 by the *New York Times*, prior to

²² Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Woke Blacks’,” UsHadrons, October 19, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-woke-blacks-d42b989ddd7f>.

²³ Jonathan Morgan and Kris Shaffer, “Sockpuppets, Secessionists, and Breitbart, How Russia May Have Orchestrated a Massive Social Media Influence Campaign,” Data for Democracy, March 31, 2017, <https://medium.com/data-for-democracy/sockpuppets-secessionists-and-breitbart-7171b1134cd5>.

the public revelations about the Internet Research Agency's role in the active measures campaign against the 2016 election.²⁴

Once the confidence of the followers of the fallacious accounts, channels, handles, and sites was gained, more weaponized messages would be distributed. A social media account whose content at one time may have been patriotic, humorous, or off color, or perhaps playing on themes in popular culture, as the 2016 election got closer, started to push messages with a more sinister purpose. Two such Russian directed Twitter accounts, "Jenna_Abrams" and "Pamela_Moore13," provided several examples of how the messaging changed over time. A few of these posts are displayed in Figures 7–19.

²⁴ Adrian Chen, "The Agency," *New York Times Magazine*, June 2, 2015, <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>.



Figure 7. Content from the Russian Social Media Site “Jenna Abrams.”²⁵

²⁵ Source: “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’,” UsHadrons, February 1, 2018, <https://medium.com/@ushadrons/this-is-space-is-a-repository-for-content-from-the-russian-twitter-account-jenna-abrams-c1570b468b86>.



Figure 8. Content from the Russian Social Media Site “Jenna Abrams.”²⁶

²⁶ Source: UsHadrons, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”



Figure 9. Content from the Russian Social Media Site “Jenna Abrams.”²⁷

²⁷ Source: UsHadrns, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”



Figure 10. Content from the Russian Social Media Site “Jenna Abrams.”²⁸

²⁸ Source: UsHadrons, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”



Figure 11. Content from the Russian Social Media Site “Jenna Abrams.”²⁹

²⁹ Source: UsHadrons, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”



Figure 12. Content from the Russian Social Media Site “Jenna Abrams.”³⁰

³⁰ Source: UsHadrns, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”



Figure 13. Content from the Russian Social Media Account “PamelaMoore13.”³¹

³¹ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Pamela_Moore13’,” UsHadrons, October 27, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-pamela-moore13-a53525a1bc38>.

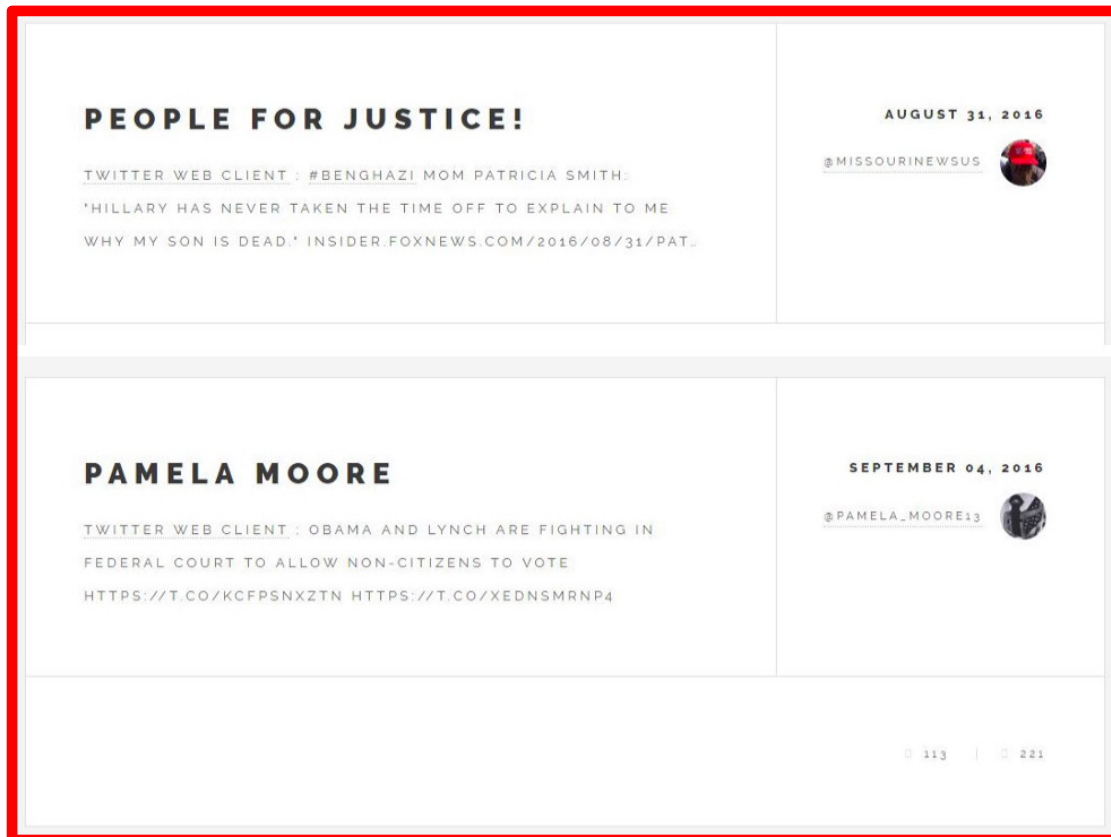


Figure 14. Content from the Russian Social Media Account “Pamela Moore13.”³²

³² Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Pamela_Moore13’.”



Figure 15. Content from the Russian Social Media Account "Pamela Moore13."³³

³³ Source: "This Space Is a Repository for Content from the Russian Social Media Account 'Pamela_Moore13'."



Figure 16. Content from the Russian Social Media Account "Pamela Moore13."³⁴

³⁴ Source: "This Space Is a Repository for Content from the Russian Social Media Account 'Pamela_Moore13'."



Figure 17. Content from the Russian Social Media Account "Pamela Moore13."³⁵

³⁵ Source: "This Space Is a Repository for Content from the Russian Social Media Account 'Pamela_Moore13'."

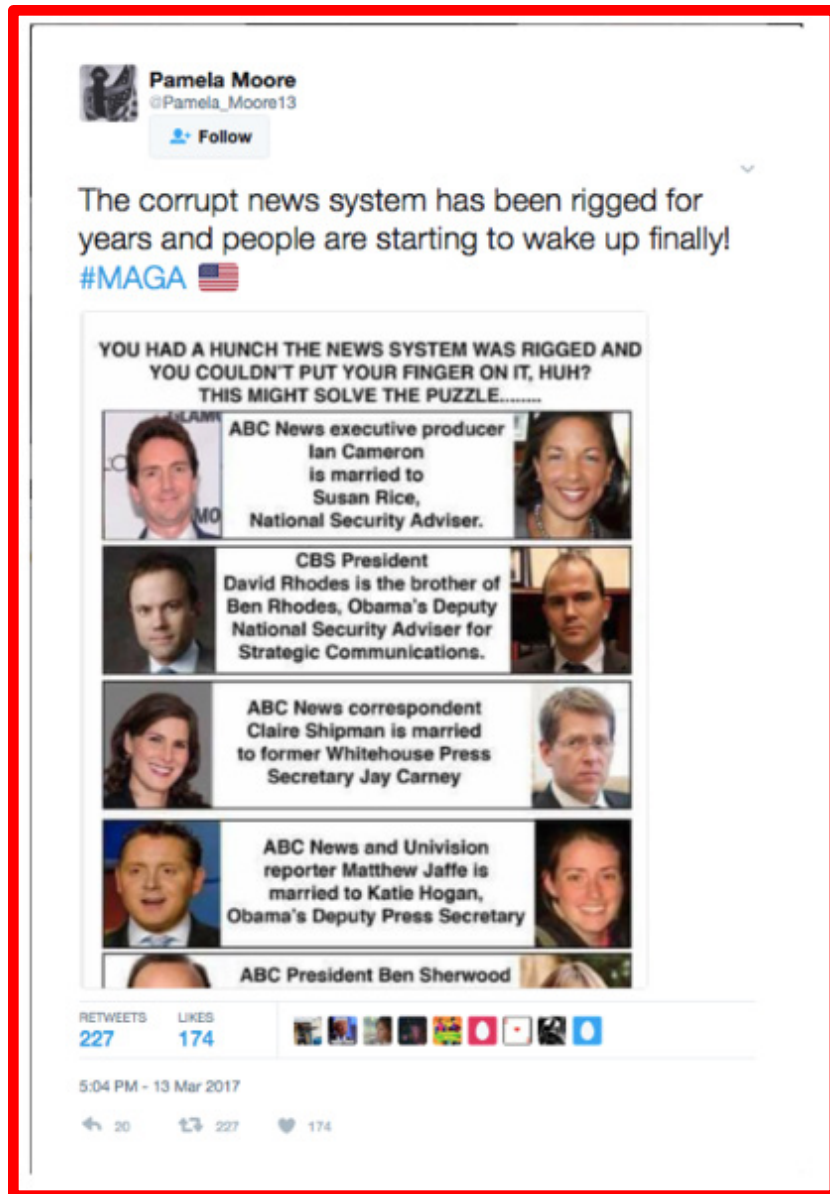


Figure 18. Content from the Russian Social Media Account “Pamela Moore13.”³⁶

³⁶ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Pamela_Moore13’.”

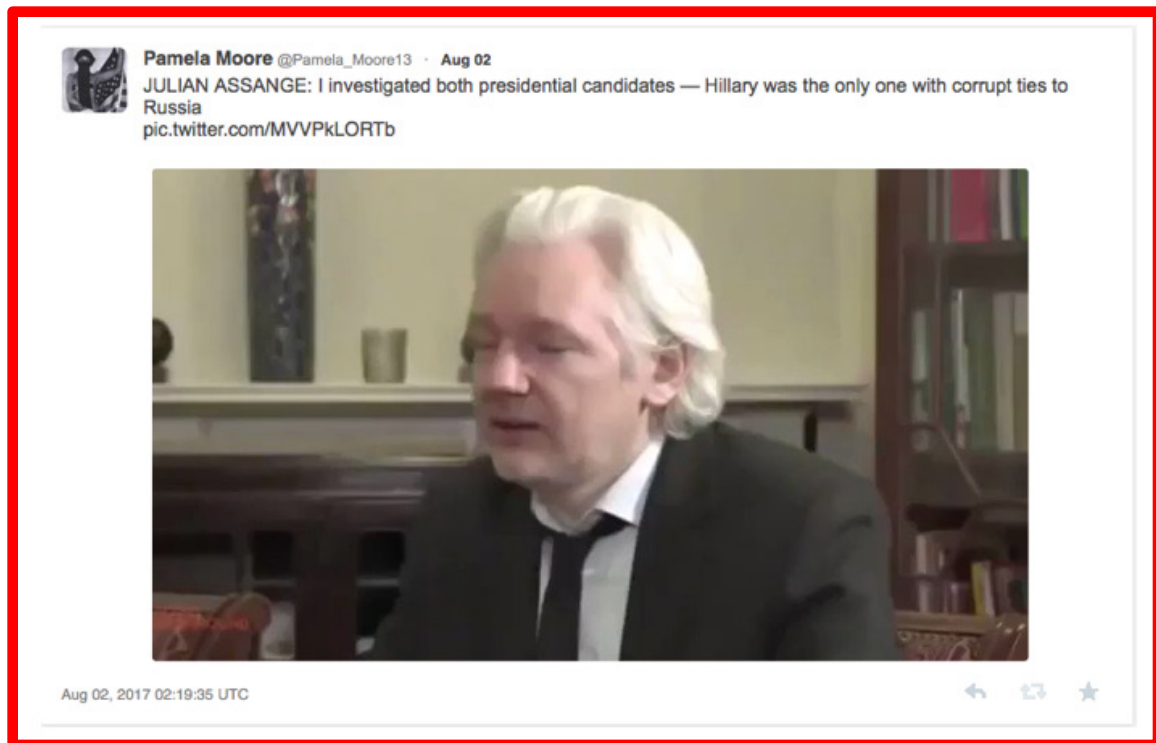


Figure 19. Content from the Russian Social Media Account “Pamela Moore13.”³⁷

Compounding the impact of the Kremlin’s tactics is research that shows that false information spreads deeper and faster over the internet than truth.³⁸ Researchers at the Massachusetts Institute of Technology (MIT) found that the difference between the diffusion of false news stories as compared to true news stories was stark. The false stories spread six times faster over the internet, reached greater depth, and a broader audience than the true stories.³⁹ The MIT research provides evidence to what political strategists have known a priori for a long time, negative narratives can take hold in a population quickly, while regardless of their veracity, once established, are very difficult to counter. Political campaigns are so willing to use negative advertising for this reason,

³⁷ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Pamela_Moore13’.”

³⁸ Soroush Vosoughi, Deb Roy, and Sinan Aral, *The Spread of True and False News Online* (Cambridge, MA: MIT Initiative on the Digital Economy, 2017), 2–3, <http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf>.

³⁹ Vosoughi, Roy, and Aral, 2–3.

and candidates who shy away from this form of political propaganda, do so at their own peril. What mainstream politics has also taught is that countering false or negative narratives is very difficult and often impossible. The simple act of rebuttal can often provide legitimacy to the false narrative and increase its lifespan in the public psyche.⁴⁰

The change in how the American public now determines facts is one of the environmental factors that has increased the effectiveness of the Kremlin's information warfare strategy. With the internet, private individuals, not professional journalists, are becoming the curators of the information they receive in a disaggregated information environment.⁴¹ This change in the media climate has permitted the Kremlin to drive its narratives farther and faster than in the past.

The chart in Figure 20 comes from a report published on the propaganda-tracking website Hamilton 68. It documents the speed with which two different propagandistic narratives spread, one in the 1980s, about an imaginary U.S. bio weapon designed to target certain ethnic populations, and a 2018 conspiracy about a U.S. project to fill drones with toxic mosquitos. According to the Hamilton 68 researchers, in the 1980s, it took seven years for the malignant story to take hold with legitimate news outlets while in 2018, the same penetration into the mainstream media took less than a month.

⁴⁰ Christopher and Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, 9.

⁴¹ Michael Dimock, "Our Expanded Focus on Trust, Facts and the State of Democracy," Pew Research Center, April 26, 2018, <http://www.pewresearch.org/2018/04/26/our-expanded-focus-on-trust-facts-and-the-state-of-democracy/>.

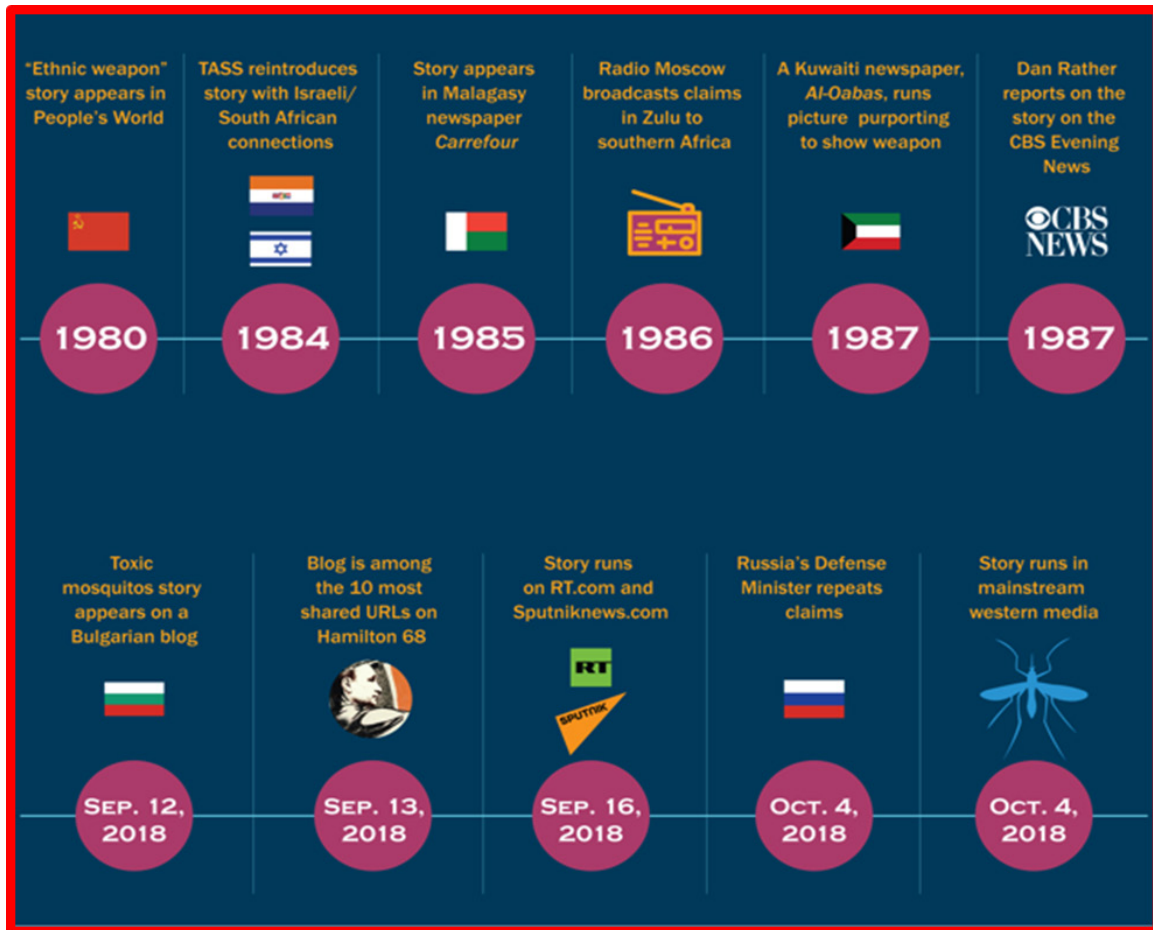


Figure 20. A Comparative Timeline of the Spread of Anti-American Rumors before and after the Advent of Social Media, as It Appeared on the Website Hamilton 68.⁴²

This shift away from traditional print and network news has been well documented. A common point of reference for making decisions critical to democracy has faded away, while along with it, the importance of evidence and facts has been diminished in shaping policy debates.⁴³ Part of the loss of a common point of reference can be attributed to how algorithms now provide people with the tailored information that these artificial minds think they want. A world has been created in which many now live

⁴² Source: Bret Schafer, "A View from the Digital Trenches—Lessons from Year One of Hamilton 68," Alliance for Security Democracy, November 2108, <https://securingdemocracy.gmfus.org/a-view-from-the-digital-trenches-lessons-from-year-one-of-hamilton-68/>.

⁴³ Dimock, "Our Expanded Focus on Trust, Facts and the State of Democracy."

in “filter bubbles,” as described by Eli Pariser, a politically left leaning internet activist.⁴⁴ While Pariser’s political background has likely influenced his perspective, his description of information bubbles, insulating readers from the divergent points of view that can create cognitive dissonance, should ring true to anyone who has experienced the narrowing on news subjects received through their smartphones or social media interface. In short, algorithms track what is viewed, then offer back information choices based on the perceived preferences. This mirrored flow of information limits perspectives and provides all individuals with their own personal information environment.⁴⁵

Research published by Stanford University in early 2019, illustrated how individuals’ political perspectives could shift back towards norms established prior to the proliferation of social media. Specifically, Stanford’s research showed how a sample group of social media users’ political views became less polarized when they abstained from their Facebook accounts.⁴⁶ The Stanford researchers noted that while the sample participants became somewhat less current on political events, their opinions began to trend back more to the traditional center of American Democratic and Republican positions. The chart in Figure 21 illustrates this trend.⁴⁷

⁴⁴ Eli Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think* (New York: Penguin Books, 2011), 1–10.

⁴⁵ Pariser, 1–10.

⁴⁶ Hunt Allcott et al., *The Welfare Effects of Social Media* (Palo Alto, CA: Stanford University, 2019), 1, <http://web.stanford.edu/~gentzkow/research/facebook.pdf>.

⁴⁷ Allcott et al., 12–13.

Figure 4: Issue Opinions by Party at Endline

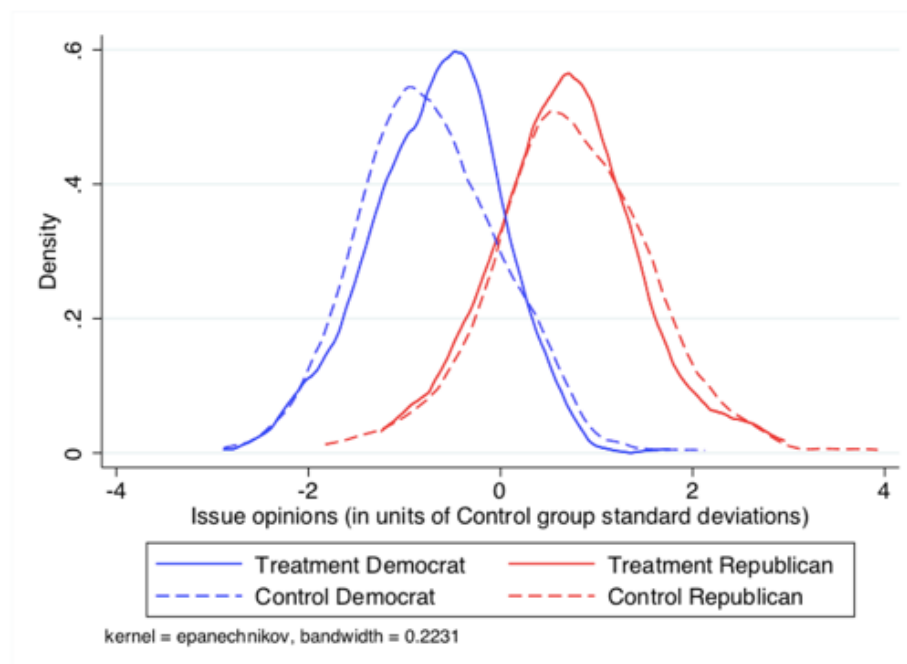


Figure 21. Normalization of Political Views with Facebook Abstinence, as Published by Stanford University.⁴⁸

B. THE 2016 U.S. PRESIDENTIAL ELECTION AND ONGOING RUSSIAN STRATEGY

In 2016, the Kremlin’s propagandist, including the Internet Research Agency, fed socially divisive, conspiratorial information to the users of social media. The DNI reported in early 2017 that Russian President Vladimir Putin ordered an influence campaign against the 2016 U.S. presidential election. According to the DNI, this active measures or influence campaign’s goal was to undermine public faith in the U.S. democratic process.⁴⁹ The DNI report stated:

Moscow’s influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt

⁴⁸ Source: Allcott et al., 53.

⁴⁹ Office of the Director of National Intelligence, *Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections,”* 2–3.

efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or “trolls.” Russia, like its Soviet predecessor, has a history of conducting covert influence campaigns focused on U.S. presidential elections that have used intelligence officers and agents and press placements to disparage candidates perceived as hostile to the Kremlin.⁵⁰

The Russian generated content in Figure 22 shows an image of 2016 presidential candidate Hillary Clinton ironically overlayed on a Soviet style propaganda poster and includes the logo of the Cable News Network.

⁵⁰ Office of the Director of National Intelligence, ii.



Figure 22. Content from the Russian Social Media Account “AmericaFirst.”⁵¹

The DNI assessment of this attack further stated, “Russian efforts to influence the 2016 U.S. presidential election represent the most recent expression of Moscow’s longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort.” While the primary agencies that contributed to the DNI’s report, the Central Intelligence Agency, National Security Agency, and Federal Bureau of Investigation, are generally held in high esteem, controversy is still ongoing regarding these findings. The polarized political environment in the United States has made constructive public dialogue and

⁵¹ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘_AmericaFirst_’,” UsHadrons, March 17, 2018, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-americafirst-a4081efeb761>.

debate around the subject difficult. Lamentably, views around the veracity of this report often breakdown along political lines and create a rift that has been further targeted by the Kremlin’s propagandists. The Russian distributed content in Figures 23 and 24 is aimed at the U.S. intelligence community.



Figure 23. Content from the Russian Social Media Account “Anonymous News.”⁵²

⁵² Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘_Anonymous_news_,’” UsHadrons, October 29, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-twitter-account-anonymous-news-fc3fb9e1bcea>.



Figure 24. Content from the Russian Twitter Account “Jenna Abrams.”⁵³

The literatures further revealed how the Kremlin targeted more than just the 2016 U.S. presidential election with social media delivered active measures. A study published by Oxford University in 2017 stated the Kremlin targeted U.S. military personnel and veterans with propaganda, conspiracy theories, and misinformation using social media networks, and in particular, Twitter and Facebook.⁵⁴ The Oxford research revealed many

⁵³ Source: UsHadrans, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”

⁵⁴ John Gallacher, *Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns against U.S. Military Personnel and Veterans* (Oxford: Oxford University, 2017), 1–6, <http://comprop.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/10/Junk-News-on-Military-Affairs-and-National-Security-1.pdf>.

of the social media messages disseminated to the U.S. military community were pro-Russian, European right wing focused, or related to far-right political movements in the United States.⁵⁵ The Internet Research Agency propaganda in Figure 25 presumably seeks to build affinity with the U.S. military community.



Figure 25. Content Refencing Deceased U.S. Navy Seal Christopher Kyle, from the Russian Social Media Account “Veterans US.”⁵⁶

The opposing view to Russian interference in the 2016 U.S. presidential election and concurrent deployment of active measures targeting the American democracy, states that the U.S. intelligence community is wrong and the interference imaginary. The Internet Research Agency contributed to this narrative with content like that appearing in Figures 26 and 27, which satirizes the Kremlin’s use of hacking to target the 2016 presidential election and its interference in the American political system.

⁵⁵ Gallacher, *Junk News on Military Affairs and National Security*.

⁵⁶ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘veterans_us’,” UsHadrons, January 30, 2018, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-veterans-us-8c1beb0aa607>.



Figure 26. Content from the Russian Twitter Account “Jenna Abrams.”⁵⁷

⁵⁷ Source: UsHadrons, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”



Figure 27. Content from the Russian Social Media Account “Pamela Moore13.”⁵⁸

The main proponents of this hoax perspective are generally from organizations aligned with the Kremlin, or who may have received benefits for the 2016 attack. In January 2018, Leslie Stahl on the CBS News’ program 60 Minutes, interviewed Margarita Simonyan, head of the Russian government directed news channel RT. During the interview, Stahl asserted that the DNI had stated the Kremlin interfered in the 2016 U.S. presidential election, to which Simonyan responded, “And you believe them. Just like you believe that there were weapons of mass destruction in Iraq. Didn’t you believe that? Continue to believe that Russian interference in American elections happened. In five years, you will know that it didn’t.” Throughout the interview, Simonyan denied Russia’s active measures campaign against the United States and made counter-

⁵⁸ Source: UsHadrons, “This Space Is a Repository for Content from the Russian Social Media Account ‘Pamela_Moore13’.”

accusations against U.S. media outlets for anti-Russian bias.⁵⁹ Regardless of the lack of factual evidence for the Kremlin's position, news outlets in the United States, as well as political officials, echo the same basic message that Russian interference in the 2016 election is a fabrication or hoax.⁶⁰ In October 2017, former Speaker of the House Newt Gingrich published an editorial on Fox News' website blaming former Secretary of State Hillary Clinton and her husband for fabricating the "so-called Russian Collusion" scandal.⁶¹ The post in Figure 28, from the Russian social media account "Ten_GOP" (which portrayed itself as representing the Republican Party in Tennessee), shows how both the Kremlin's influence agents and U.S. media outlets contributed to the same hoax perspective. It also exemplifies the active measures strategy for amplifying messaging from other media sources.

⁵⁹ Lesley Stahl, "RT's Editor-In-Chief on Election Meddling, Being Labeled Russian Propaganda," CBS, January 7, 2017, <https://www.cbsnews.com/news/rt-editor-in-chief-on-election-meddling-russian-propaganda-label/>.

⁶⁰ Angie Drobnic Holan, "2017 Lie of the Year: Russian Election Interference a Made-Up-Story," Politifact, December 12, 2017, <https://www.politifact.com/truth-o-meter/article/2017/dec/12/2017-lie-year-russian-election-interference-made-s/>.

⁶¹ Newt Gingrich, "The Clinton Started the so-called Russian Collusion Scandal and May be Destroyed by It," Fox News, October 27, 2017, <https://www.foxnews.com/opinion/newt-gingrich-the-clintons-started-the-so-called-russian-collusion-scandal-and-may-be-destroyed-by-it>.

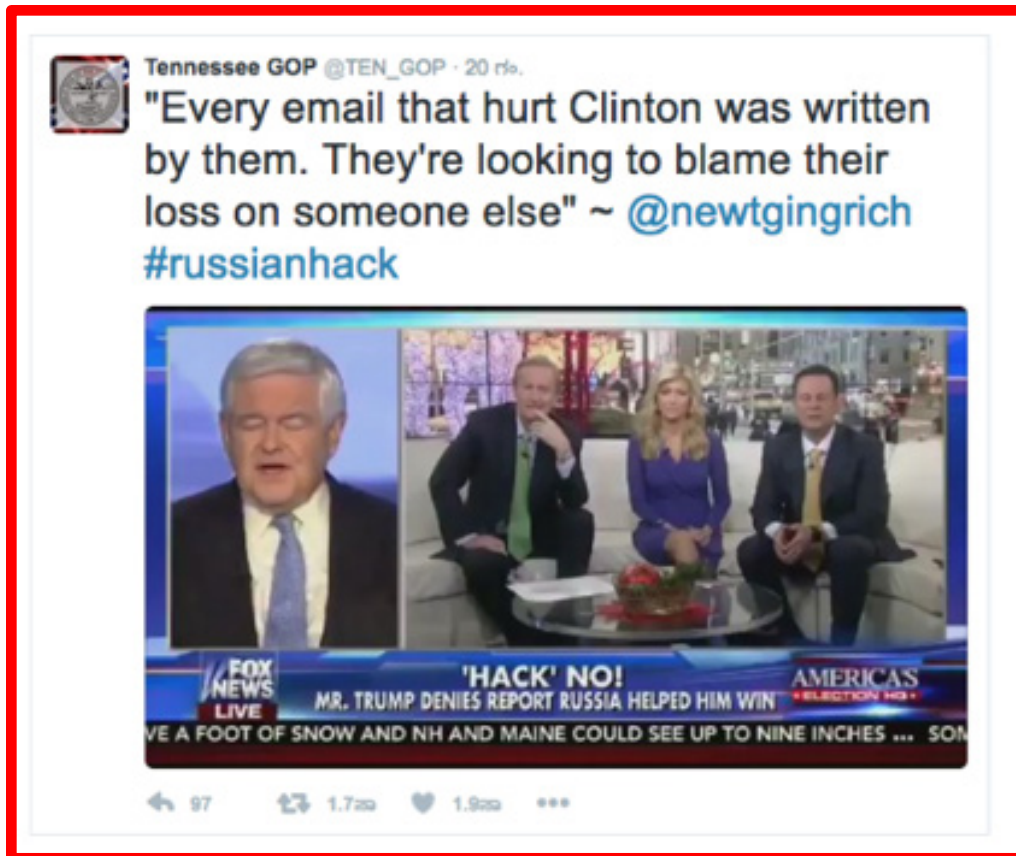


Figure 28. Content from the Russian Twitter Account “TEN GOP.”⁶²

As a counterpoint to the hoax narrative, congressional leaders from both the Democratic and Republican parties in the United States have supported investigations into Russia’s interference in U.S. democratic processes. A bi-partisan report issued by the Senate Select Committee on Intelligence, released July 3, 2018, corroborated the DNI’s 2017 assessment of the Kremlin’s active measures campaign. The Senate’s findings emphasized the veracity and seriousness of the Kremlin’s 2016 attack on the U.S. democracy, while encountering no evidence of political bias in the original intelligence community report. Nevertheless, the Senate also stated, “the Committee’s investigation has exposed a far more extensive Russian effort to manipulate social media outlets to sow

⁶² Source: “This Space Is a Repository for Content from the Russian Twitter Account ‘Ten_GOP’,” UsHadrns, October 19, 2017, <https://medium.com/@ushadrns/this-space-is-a-repository-for-content-from-the-russian-social-media-account-ten-gop-ed7e6cf6d30>.

discord and to interfere in the 2016 election and American society.”⁶³ While the original intelligence assessment references social media manipulation, and in particular, the Kremlin directed Internet Research Agency, the Senate’s analysis concluded that Russian social media exploitation was far greater than described by the DNI in 2017.

Nevertheless, none of the documents supporting the presence of Russian active measures in the 2016 election stated that the Russians created the environment into which they planted their seeds of division. Racism, xenophobia, intolerance, gun violence, crime, homophobia, Islamophobia, and anti-government extremism, were already part of American discourse. As these tears already existed in the U.S. social fabric, all Moscow’s propagandist did was pull on the threads, but to what effect? As to swinging the election for one candidate or the other, and thus, directly impacting the U.S. democracy, the DNI report did not cover the subject. Furthermore, this research has revealed little statistical evidence showing the impact of the Kremlin’s ongoing active measures campaigns.

C. COMBATING INFLUENCE OPERATIONS/STRENGTHENING DEMOCRACY

As documented by *The Economist* in a June 2013 article, the model Vladimir Putin’s Russia seeks to replace western freedom with, from physical space to cyberspace, is authoritarian and dictatorial, where truth is irrelevant and government control absolute.⁶⁴ This description draws sharp parallels to images in worlds described in the classic dystopian novels *1984* by George Orwell and *Brave New World* by Aldous Huxley.⁶⁵ While the former points to information control in a totalitarian society, and the latter, information profusion, they both emphasize the linkage between propaganda and population manipulation.

From the Cold War until today, the U.S. government has focused on countering Soviet and Russian anti-western, antidemocratic, totalitarian messaging with media

⁶³ Senate Select Committee on Intelligence, *The Intelligence Community Assessment*, 3–4.

⁶⁴ “Putin’s Russia: Repression Ahead,” *The Economist* 407, no. 8838 (June 1, 2013), <https://www.economist.com/europe/2013/06/01/repression-ahead>.

⁶⁵ George Orwell, *1984: A Novel* (New York: Signet Classic, 1977), 1–331; Aldous Huxley, *Brave New World* (New York: Bantam Books, 1958), 1–239.

outlets, such as *Voice of America* and Radio Free Europe, but the target audiences are foreign not domestic. Nevertheless, a large body of academic writing is available on European democracies and their experience in defending their populations against Russian influence operations. Some of the techniques developed in Europe, particularly in the Nordic nations, may be applicable to the United States. In June 2017, Janis Sarts, Director of the NATO Strategic Communications Center of Excellence, testified to the U.S. Senate. His first recommendation for combating active measures through cyber space was raising society's awareness. Sarts stated:

As has been described before, society and its perceptions are the main targets of the contemporary influence operations. Accordingly, one of the key resilience mechanisms, our research shows, is awareness of the society of being targeted by third party malicious actors to affect their election behavior. We have seen resilience levels raise instantly as society recognizes being targeted by outside actor.⁶⁶

Sarts' testimony emphasized the importance of educating populations about the threat from influence operations.⁶⁷

Another point emphasized in the literature reviewed was the importance of supporting and strengthening democratic institutions while fighting corruption. *The Kremlin Playbook*, a document produced by the Center for Strategic and International Studies (CSIS) in 2016, emphasized the continued need to respond to the effects of Russia's active measure campaigns with open, transparent, and democratic practices.⁶⁸ According to *The Kremlin Playbook*, "Because corruption plays a central role in sustaining and propagating Russian influence, it is essential to stop the virus's transmission mechanism. Corruption is enabled by a lack of transparency as well as institutional opaqueness and dysfunction, allowing these networks to operate and grow undetected until the body is overcome."⁶⁹ The link between fighting corruption while

⁶⁶ *Russian Intervention in European Elections: United States Senate Select Committee on Intelligence*, Senate, 115th Cong., 1st sess., June 28, 2017, 5, <https://www.intelligence.senate.gov/sites/default/files/documents/sfr-jsarts-062817b.pdf>.

⁶⁷ S., *Russian Intervention in European Elections*, 1–7.

⁶⁸ Heather Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Lanham, MD: Rowman and Littlefield, 2016), 26–34.

⁶⁹ Conley et al., 27.

blunting the transmission of propaganda was reflected in multiple documents examined. The impact and applicability of anticorruption practices for an established democracy like the United States, as compared to the emerging democracies of the former Soviet Union is probably different. Nevertheless, being open with the American people about Russian involvement in the 2016 election, as well as ongoing active measures operations, would fall in line with the transparency recommended by CSIS.

D. TRACKING THE BOTS AND TROLLS

To combat an enemy, it is necessary to know when, where, and how the adversary is operating; the literature implies that these requirements also are valid for cyber strategic weapons of influence. An emerging field is the tracking of influence campaigns on social media. The Alliance for Securing Democracy, a NGO based at the German Marshall Fund in the United States, has set up a Russian disinformation bot tracking website for Twitter called *Hamilton 68*. The site is named for Alexander Hamilton's Federalist Papers No. 68, which refers to protecting America's electoral process from foreign interference. Part of the site's introductory narrative states, "We are not telling you what to think, but we believe you should know when someone is trying to manipulate you. What you do with that information is up to you."⁷⁰ The site lists 600 Twitter accounts it monitors linked to Russian influence operations and contains charts and graphics for multiple Twitter related data points, like top hashtags. Another website article from Robhat Labs provided background and analysis on a propaganda bot tracking program that also focused on Twitter. The Robhats Labs article describes using an algorithm to track political propaganda bots and a classifier to look at patterns.⁷¹ While it did not look specifically at Russian propaganda or active measures, the tools and techniques could potentially be overlaid for this purpose.

⁷⁰ Laura Rosenberg and J. M. Berger, "Hamilton 68: A New Tool to Track Russian Disinformation on Twitter," Alliance for Security Democracy, August 2, 2017, <https://securingdemocracy.gmfus.org/hamilton-68-a-new-tool-to-track-russian-disinformation-on-twitter/>.

⁷¹ "An Analysis of Propaganda Bots on Twitter," Robhat Labs, October 30, 2017, <https://medium.com/@robhat/an-analysis-of-propaganda-bots-on-twitter-7b7ec57256ae>.

A third ongoing research program reviewed is *The Computational Propaganda Project* out of Oxford University in England. This project's homepage states it aims to, "investigates the interaction of algorithms, automation and politics. This work includes analysis of how tools like social media bots are used to manipulate public opinion by amplifying or repressing political content, disinformation, hate speech, and junk news."⁷² The Oxford project looks at political manipulation through social media in several nations. A research paper released under the project's banner in July 2018 took a deeper look at the evidence that automated social media traffic was being used to degrade democracy and social discourse.⁷³ In December 2018, the project published its findings into Russian generated social media content as provided by the Senate Select Committee on Intelligence. Of note, this research found, "these campaigns did not stop once Russia's IRA was caught interfering in the 2016 election. Engagement rates increased and covered a widening range of public policy issues, national security issues, and issues pertinent to younger voters."⁷⁴ The authors noted and corroborated the official U.S. intelligence community findings that the Kremlin's propagandists sought to interfere not just in the U.S. 2016 election, but to polarize the U.S. public. It specifically named tactics aiming to discourage African American voter participation and increase Hispanic American distrust in government institutions, while also to encourage extreme right-wing voters to be more confrontational.⁷⁵ The Russian deseminated social media content in Figures 29–45 show the aggressive nature of the Kremlin's campaign.

⁷² "The Computational Propaganda Project: Algorithms, Automation and Digital Politics," Oxford University, last modified July 20, 2018, <http://comprop.oii.ox.ac.uk>.

⁷³ Samantha Bradshaw and Philip Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation* (Oxford: Oxford University, 2018), 3, <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf>.

⁷⁴ Philip Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012–2018* (Oxford: Oxford University, 2018), 3, <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf>.

⁷⁵ Howard et al., 3.

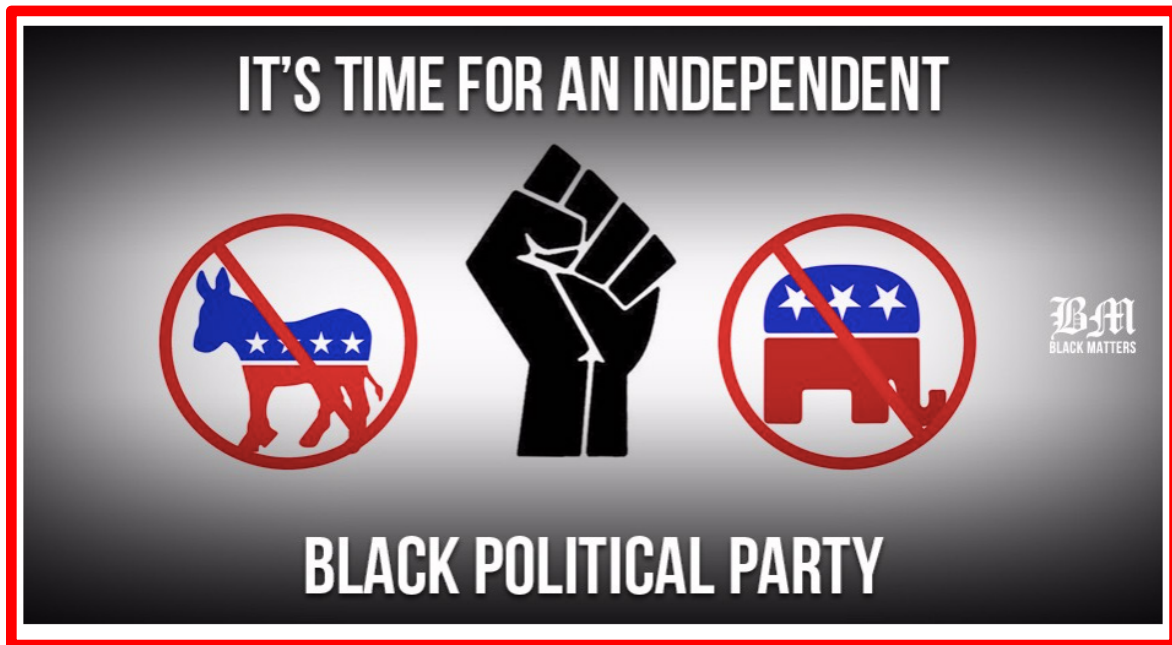


Figure 29. Content from the Russian Instagram Account “Black Matters.”⁷⁶

⁷⁶ Source: UsHadrons, “This Space Is a Repository for Content from the Russian Social Media Account ‘Watch.the.Police’.”



Figure 30. Content from the Russian Social Media Account “USA Gunslinger.”⁷⁷

⁷⁷ Source: UsHadrons, “This Space Is a Repository for Content from the Russian Twitter Account ‘USA_Gunslinger’.”

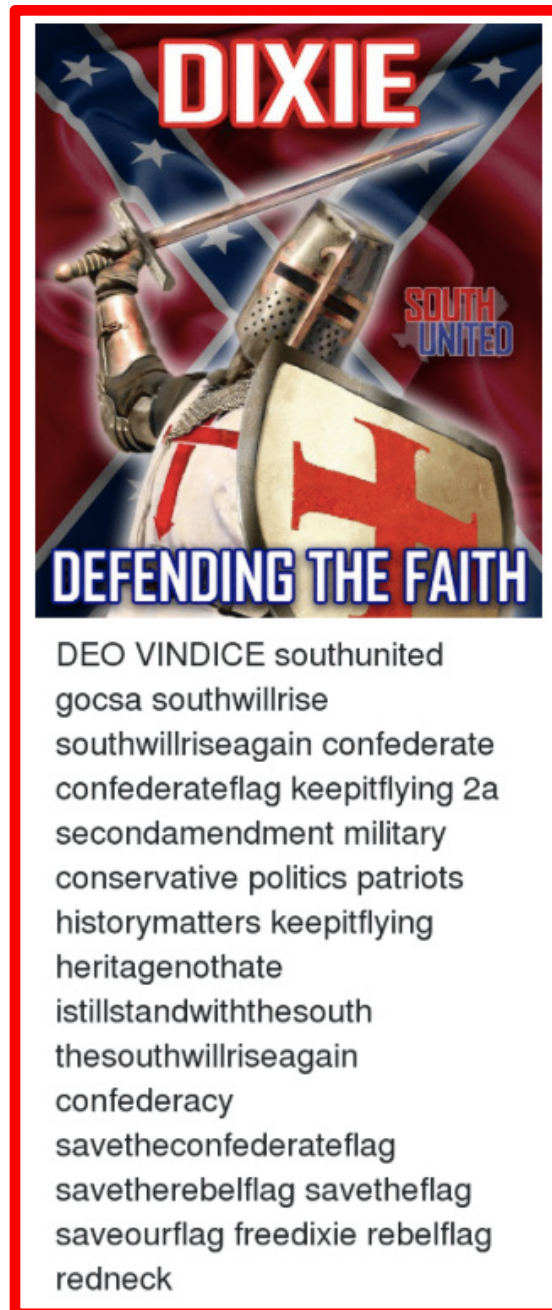


Figure 31. Content from the Russian Social Media Account “South United.”⁷⁸

⁷⁸ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘South United’,” UsHadrons, October 17, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-south-united-35bcdea6f29>.



Figure 32. Content from the Russian Social Media Account “Woke Blacks.”⁷⁹

⁷⁹ Source: UsHadrons, “This Space Is a Repository for Content from the Russian Social Media Account ‘Woke Blacks’.”



Figure 33. Content from the Russian Social Media Account "Secure Borders."⁸⁰

⁸⁰ Source: "This Space Is a Repository for Content from the Russian Social Media Account 'Secured Borders'," UsHadrans, October 12, 2017, <https://medium.com/@ushadrans/this-space-is-a-repository-for-ads-from-the-russian-social-media-group-secured-borders-a62acfa7726>.



Figure 34. Content from the Russian Social Media Account “Secure Borders.”⁸¹

⁸¹ Source: UsHadrons, “This Space Is a Repository for Content from the Russian Social Media Account ‘Secured Borders’.”



Figure 35. Content from the Russian Social Media Account “Army of Jesus.”⁸²

⁸² Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Army of Jesus’,” UsHadrons, October 18, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-army-of-jesus-553c6aa74fea>.



Figure 36. Content from the Russian Social Media Account Stop All Invaders.”⁸³

⁸³ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Stop All Invaders,’” UsHadrons, October 17, 2017, <https://medium.com/@ushadrons/stop-the-invasion-f8c93d774f97>.



Figure 37. Content from the Russian Social Media Accounts “Merican Fury.”⁸⁴

⁸⁴ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘MericanFury’,” UsHadrons, October 25, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-mericanfury-7066546c96b>.



Figure 38. Content from the Russian Social Media Account "Stop All Invaders."⁸⁵

⁸⁵ Source: USHadrons, "This Space Is a Repository for Content from the Russian Social Media Account 'Stop All Invaders'."

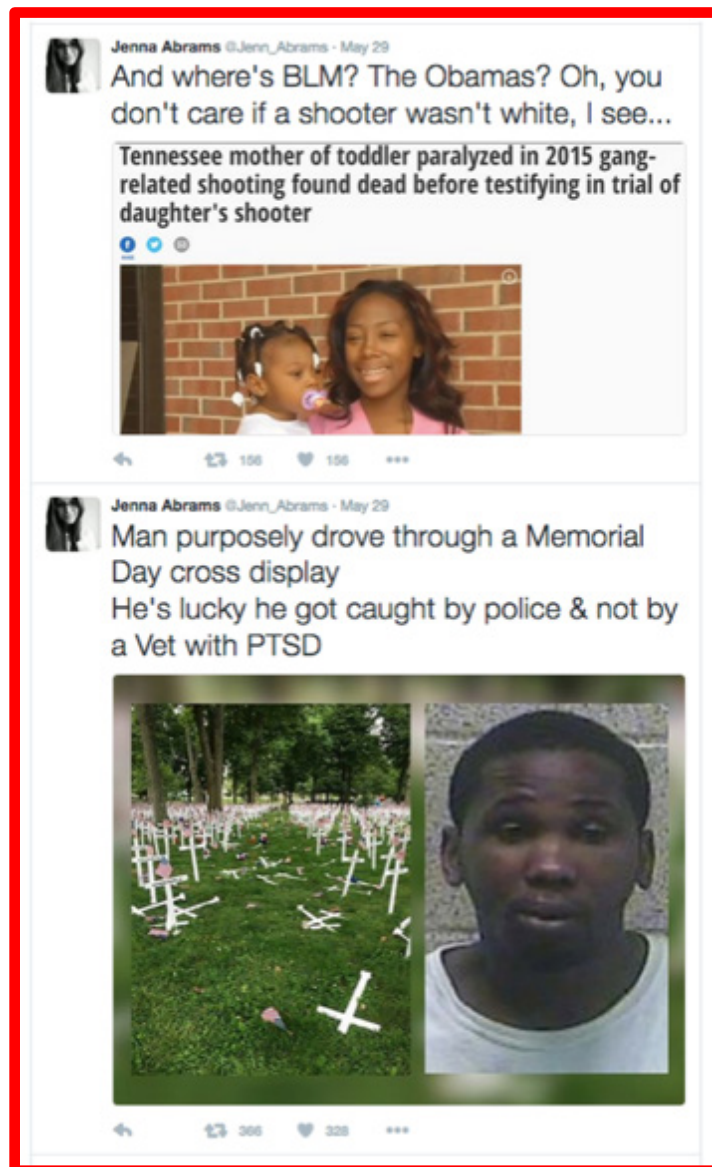


Figure 39. Content from the Russian Twitter Account “Jenna Abrams.”⁸⁶

⁸⁶ Source: UsHadrns, “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.”



Figure 40. Content from the Russian Social Media Account “Born Liberal.”⁸⁷

⁸⁷ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Born Liberal’,” UsHadrans, October 20, 2017, <https://medium.com/@ushadrans/this-space-is-a-repository-for-content-from-the-russian-social-media-account-born-liberal-c55ae301335c>.



Figure 41. Content from the Russian Social Media Account “Muslim Voice.”⁸⁸

⁸⁸ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Muslim_Voice’,” UsHadrons, October 23, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-muslim-voice-b22bf2bc1c57>.



Figure 42. Content from the Russian Social Media Account “Rainbow Nation US.”⁸⁹

⁸⁹ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Rainbow_Nation_US’,” UsHadrans, October 22, 2017, <https://medium.com/@ushadrans/this-space-is-a-repository-for-content-from-the-russian-social-media-group-rainbow-nation-us-cc30ba458951>.

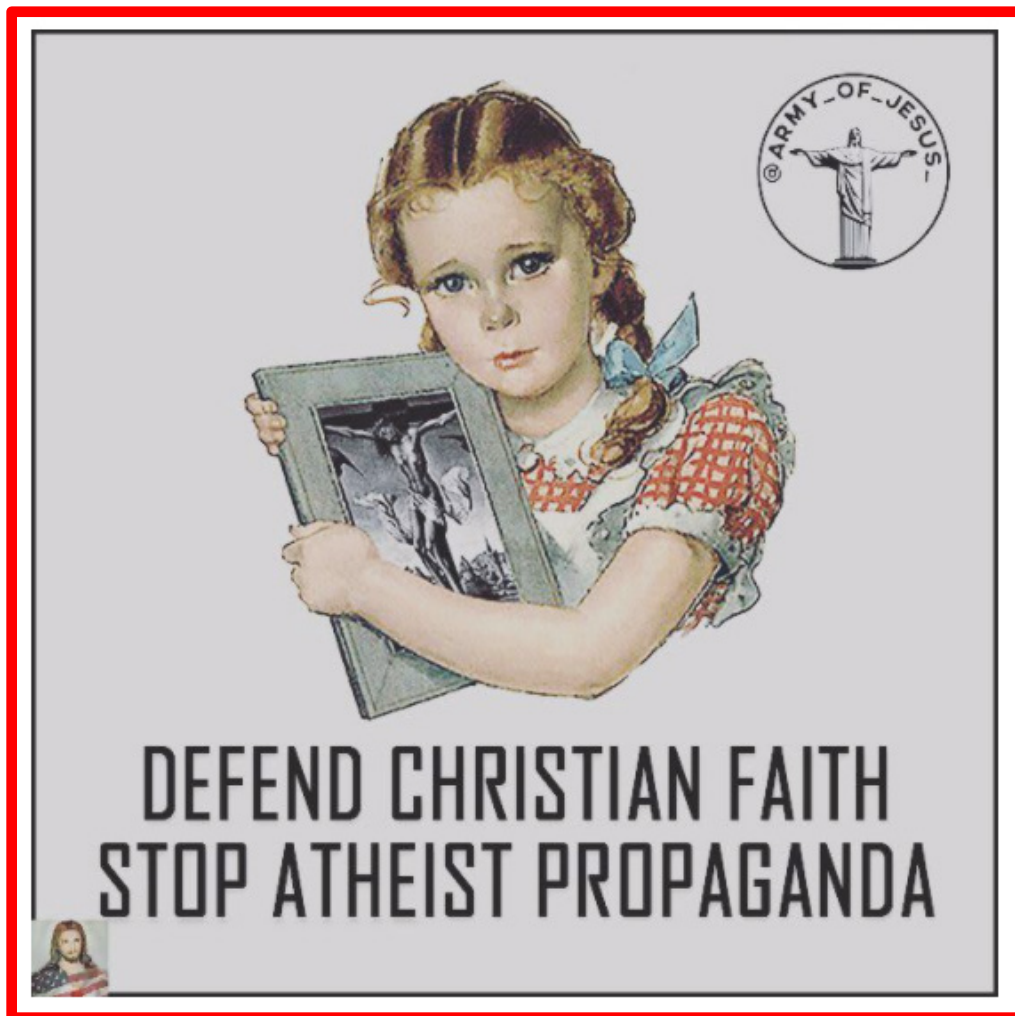


Figure 43. Content from the Russian Social Media Account “Army of Jesus.”⁹⁰

⁹⁰ Source: UsHadrons, “This Space Is a Repository for Content from the Russian Social Media Account ‘Army of Jesus’.”

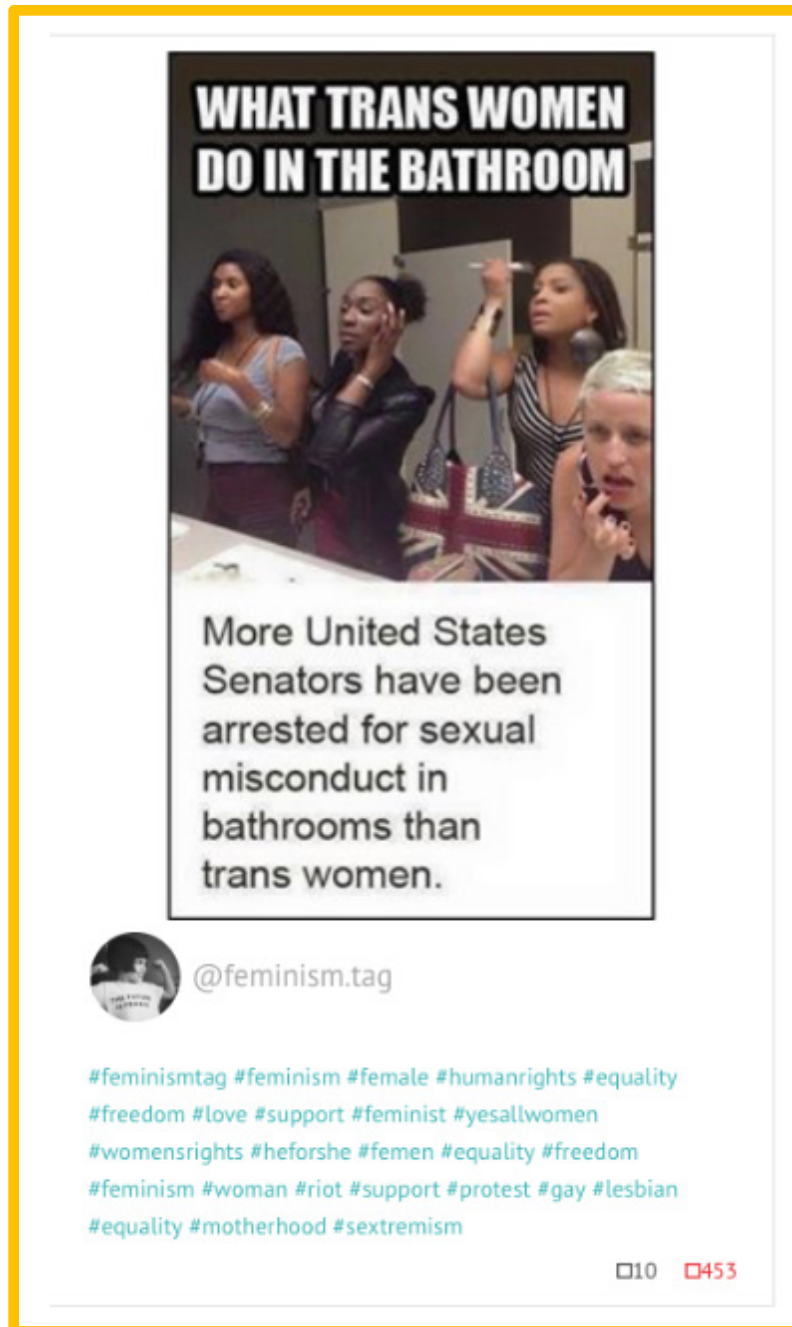


Figure 44. Content from the Russian Social Media Account “Feminism Tag.”⁹¹

⁹¹ Source: “This Space Is a Repository for Content from the Russian Social Media Account ‘Feminism Tag,’” UsHadrons, October 22, 2017, <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-feminism-tag-24b2cf5a3525>.

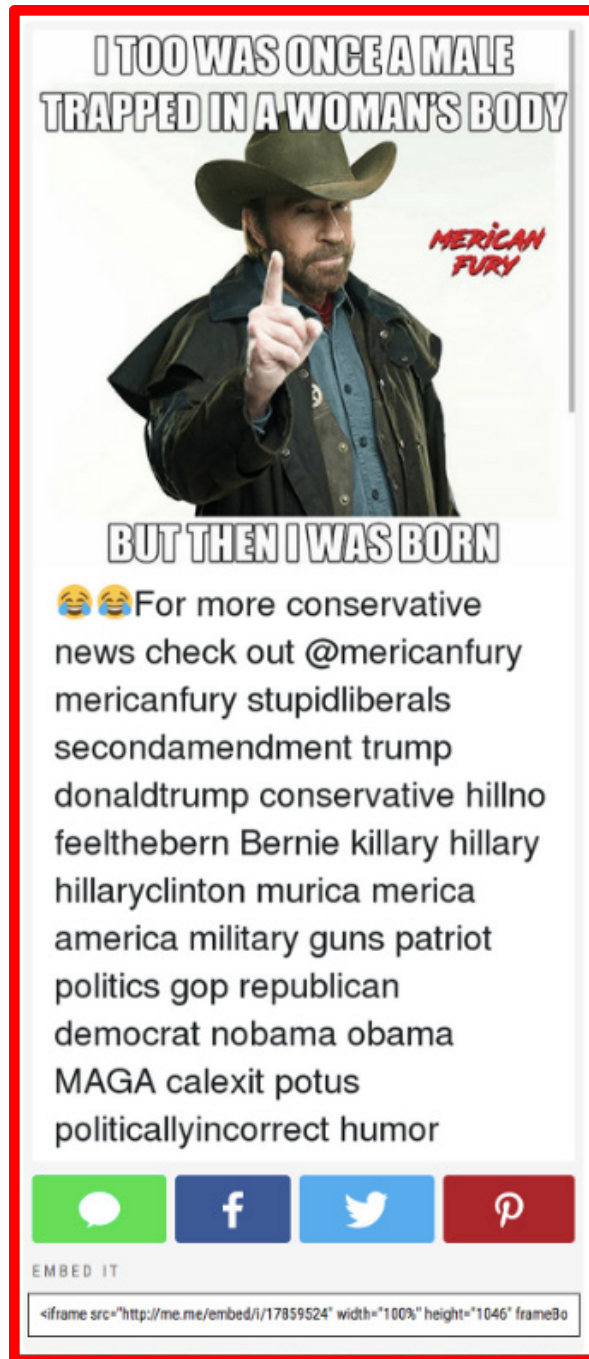


Figure 45. Content from the Russian Social Media Account “Merican Fury.”⁹²

⁹² Source: USHadrons, “This Space Is a Repository for Content from the Russian Social Media Account ‘MericanFury’.”

E. THE PRESENT RESPONSE, GOVERNMENTAL, AND CORPORATE

Multiple documents reviewed reveal that since late 2016, the U.S. government and social media companies have responded to the Kremlin's active measures campaign in various ways. Republicans and Democrats in the Senate and House of Representatives proposed the bi-cameral, bi-partisan Honest Ads Act in October 2017. The act would apply Federal Communications Commission advertisement transparency rules to social media platforms. According to its congressional sponsors, this act ensures companies, like Facebook, Twitter, and Google, obtain information from the purchasers, and then record the costs, audiences targeted, as well as which candidate or issue is the subject of the advertising.⁹³ The act's theory, according to a report in *The Hill* from October 2017, is that its policies will provide enough information for the American people to identify those seeking to influence their vote, while further aiding government agencies in determining what advertising constitutes foreign interference in U.S. politics.⁹⁴ By spring 2018, both Facebook and Twitter had endorsed the Honest Ads Act. Facebook CEO Mark Zuckerberg stated on April 6, 2018, "Election interference is a problem that's bigger than any one platform, and that's why we support the Honest Ads Act. This will help raise the bar for all political advertising online."⁹⁵ As of January 2019, the Honest Ads Act had not been signed into law; therefore, data was not available to determine its impact.

The literature further shows the U.S. government's legislative and executive branches have imposed economic sanctions on Russian businesses and private citizens linked to the Kremlin's attempts to interfere in U.S. internal affairs. As documented by a *New York Times* article in late 2016, the U.S. Department of State took measures against Russian diplomats, 35 of which were expelled from the United States and listed as

⁹³ Honest Ads Act, H. Res. 4077, House of Representatives, 115th Cong., 1st sess., 2017–2018, <https://www.congress.gov/bill/115th-congress/house-bill/4077/text>.

⁹⁴ Timothy Roemer and Zachary Wamp, "This Is the Best First Step to Stop Russian Meddling in Our Politics," *The Hill*, October 26, 2017, <http://thehill.com/opinion/national-security/357238-this-is-the-best-first-step-to-stop-russian-meddling-in-our>.

⁹⁵ Mark Zuckerberg, "Mark Zuckerberg," Facebook, April 6, 2018, <https://www.facebook.com/zuck/posts/10104784125525891>.

persona non grata.⁹⁶ The U.S. Department of Treasury undertook another notable punitive action in March 2018 when it placed economic sanctions of various Russian entities for destructive and destabilizing cyber activities. In a press release, Treasury officials stated, “targeted sanctions are a part of a broader effort to address the ongoing nefarious attacks emanating from Russia” and that the sanctions were an action that “counters Russia’s continuing destabilizing activities, ranging from interference in the 2016 U.S. election to conducting destructive cyber-attacks.”⁹⁷ Additionally, in late July 2018, according to a U.S. Department of Justice press release, 12 Russian nationals were charged for “committing federal crimes that were intended to interfere with the 2016 U.S. presidential election.”⁹⁸ Among the charges listed was the stealing of emails from the Democratic National Committee later released and used for propagandistic purposes through fictitious social media accounts created by Russia.⁹⁹ While little academic writing or research is yet available on the impact of sanctions and expulsions related to the Kremlin’s 2016 operation, future analysis should be pursued.

Starting in 2017, the U.S. Congress held multiple hearings investigating the role social media companies played in distributing Moscow’s messages, with a focus on Facebook, Twitter, Instagram, and YouTube. Partially, because of the investigations by Congress, the large social media companies have made voluntary changes to their platforms’ security procedures. These changes include how platforms usage is monitored, how customer data is collected and then distributed for exploitation (commercial or otherwise), and how automated bot driven content is detected. The *Washington Post* obtained data that showed Twitter had taken down 70 million suspicious accounts in May and June 2018. The *Post* article claimed the Twitter effort was an escalation in the social

⁹⁶ David Sanger, “Obama Strikes Back at Russia for Election Hacking,” *New York Times*, December 29, 2016, <https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html>.

⁹⁷ “Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks,” Department of Treasury, March 15, 2018, <https://home.treasury.gov/news/press-releases/sm0312>.

⁹⁸ “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,” Department of Justice, July 13, 2018, <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>.

⁹⁹ Department of Justice.

media company's "battle against fake and suspicious accounts" and "a major shift to lessen the flow of disinformation on the platform."¹⁰⁰ A *Bloomberg News* article further noted Facebook alone increased its security group by 20,000 employees as part of a commitment made during Senate hearings on the 2016 election.¹⁰¹

F. CONCLUSIONS FROM LITERATURE

The consistent takeaway from the literature reviewed for this thesis was the serious challenge the United States faces when confronting strategic weapons of influence. The documents showed the Kremlin as an adversary who has put years of practice into refining its techniques for mass psychological manipulation. Russia conceptualized deploying a weapon developed in the 20th century while exploiting present day social media, which culminated in a large-scale attack on the 2016 presidential election.

The literature further showed how multiple segments of civil society; government, private sector, academia, and NGOs, have responded to this attack. These various responses ranging from criminal investigations to social media propaganda tracking projects highlighted the progress made by combating this threat. However, the literature also revealed areas not yet addressed for combating this threat. Strategies were recommended throughout the documents reviewed to lessen the impact of strategic weapons of influence. The following are a few standouts. First, the government should take the lead in alerting the American public when this type of threat is present. Second, educational curricula should be developed that focus on building cognitive defenses against propagandistic manipulation. Third, combating this effort will require the engagement of multiple sectors of civil society.

¹⁰⁰ Craig Timberg and Elizabeth Dwoskin, "Twitter is Sweeping out Fake Accounts like Never before: Putting User Growth at Risk," *Washington Post*, July 6, 2018, https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.d1ef26563774.

¹⁰¹ Sarah Frier, "Facebook Says it Will Double Safety and Security Staff to 20,000," *Bloomberg News*, October 31, 2017, <https://www.bloomberg.com/news/articles/2017-10-31/facebook-says-it-will-double-safety-and-security-staff-to-20-000>.

III. THE KREMLIN'S SOCIAL MEDIA ATTACK ON THE 2016 U.S. PRESIDENTIAL ELECTION—A DIAGNOSIS

A. LAYERS OF DECEPTION

To understand the nature of the Kremlin's active measures campaign to influence the U.S. election through social media, it is best to take a step back and look at the overall media environment online as it pertains to misinformation. In an article published in the Harvard Kennedy School's *First Draft*, author Claire Wardle breaks down the different types of misinformation and disinformation on the internet into seven distinct types:

1—Satire or parody: no intention to harm but has the potential to fool.

2—False connection: when headlines, visuals, or captions do not support the content.

3—Misleading content: misleading use of information to frame an issue or individual.

4—False context: when genuine content is shared with false contextual information.

5—Imposter content: when genuine sources are impersonated.

6—Manipulated content: when genuine information or imagery is manipulated to deceive.

7—Fabricated content: new content is 100% false, designed to deceive and do harm.¹⁰²

Wardle then presented these categories in a matrix along with the probable motivations for their production. Figure 46 is the misinformation matrix as it appears in *First Draft*.¹⁰³

¹⁰² Claire Wardle, "Fake News: It's Complicated," *First Draft*, February 16, 2017, <https://firstdraftnews.org/fake-news-complicated/>.

¹⁰³ Wardle.

FIRSTDRAFT		MISINFORMATION MATRIX					
	 SATIRE OR PARODY	 FALSE CONNECTION	 MISLEADING CONTENT	 FALSE CONTEXT	 IMPOSTER CONTENT	 MANIPULATED CONTENT	 FABRICATED CONTENT
POOR JOURNALISM		✓	✓	✓			
TO PARODY	✓				✓		✓
TO PROVOKE OR TO 'PUNK'					✓	✓	✓
PASSION				✓			
PARTISANSHIP			✓	✓			
PROFIT		✓			✓		✓
POLITICAL INFLUENCE			✓	✓		✓	✓
PROPAGANDA			✓	✓	✓	✓	✓

Figure 46. Types of Misinformation/Disinformation as Listed in Harvard's *First Draft*.¹⁰⁴

Wardle continues to explain in more detail the dissemination mechanism for content, and acknowledges the presence of sophisticated bot driven networks and trolls that support disinformation campaigns. She discusses the psychological vulnerability of readers to these attacks, in particular how coordinated and consistent messages easily fool the human brain.¹⁰⁵ This manipulation is more easily achieved in a mass media environment where people are already exhausted by an overwhelming amount of information. These conditions have provoked a reliance on heuristics or mental shortcuts that the brain uses to establish credibility in a message by connecting the repetition of a message with veracity. As such, Wardle recommends that people double check sources before forwarding or sharing a post, video, or image, so as not to add to this information chaos.¹⁰⁶

¹⁰⁴ Source: Wardle.

¹⁰⁵ Wardle.

¹⁰⁶ Wardle.

B. ATTACKS ON REASON

The Digital Forensics Research Lab posted the graphic in Figure 47 in an article from April 2018. It highlights the logical fallacies the Kremlin uses to seed its narrative and spread disinformation.

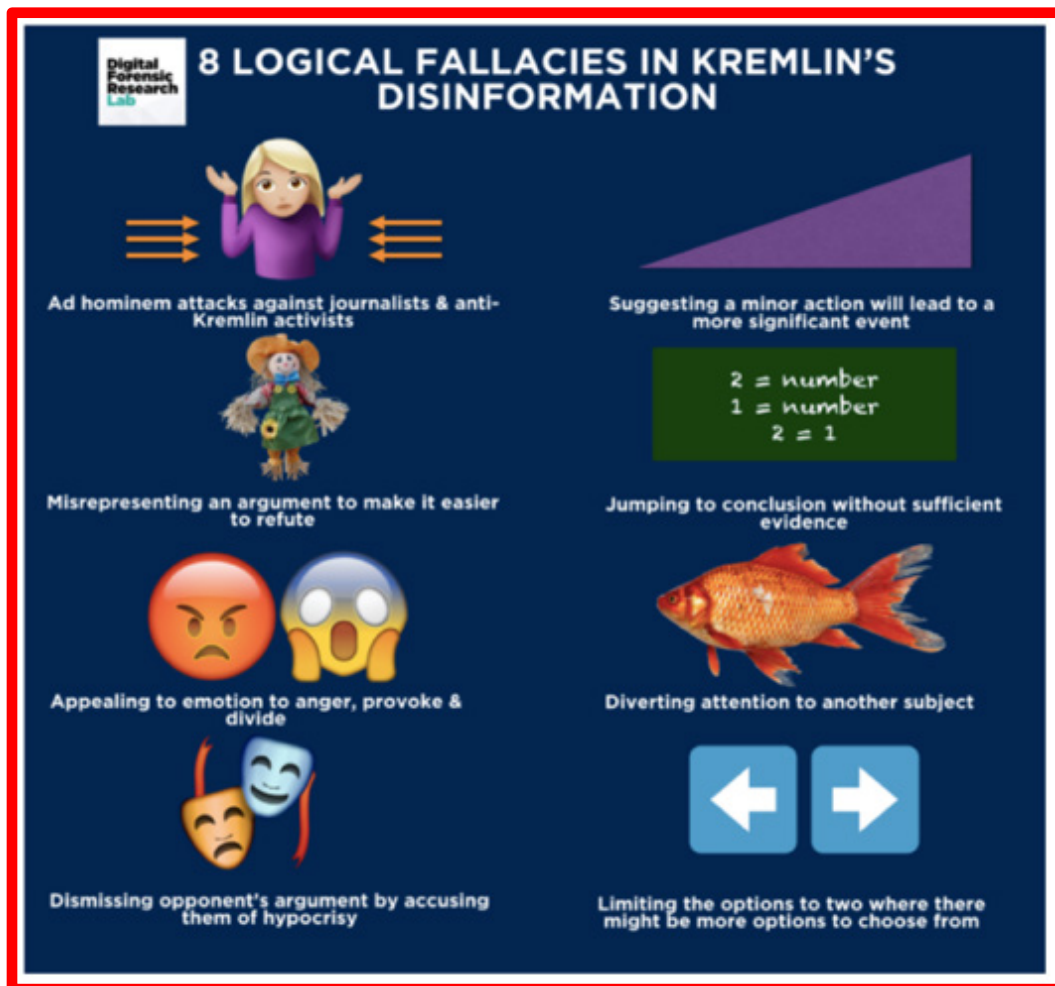


Figure 47. Graphic Displaying Logical Fallacies from the Digital Forensic Research Lab.¹⁰⁷

¹⁰⁷ Source: “Logical Fallacies Fuel Kremlin Disinfo: How the Kremlin and its Disinformation Networks Use Logical Fallacies to Dismiss, Dismay, Distract and Distort,” Digital Forensic Research Lab, April 22, 2018, <https://medium.com/dfrlab/logical-fallacies-fuel-kremlin-disinfo-e4185bb455e6>.

The fallacies utilized by the Russians can be described as ad hominem, straw man, appeal to emotion, appeal to hypocrisy, slippery slope, hasty generalization, red hearing and either/or.¹⁰⁸ While the article singles out the Kremlin for using these tactics in its propaganda operations, for anyone who has watched pundits debate on cable news, these strategies are not restricted to a singular Slavic nation. In fact, these fallacies are utilized by the greater information laundering industry.¹⁰⁹

C. INFORMATION WEAPON DEPLOYMENT

Various investigative organizations have looked at how the Kremlin's operation worked in 2016. Of particular interest was the ability to amplify damaging narratives against the campaign of Hillary Clinton at moments when the Trump campaign was being hindered by negative news coverage. The associated press did an analysis of how this counter messaging was deployed by the Kremlin's social media propagandists stating it this way, "Disguised Russian agents on Twitter rushed to deflect scandalous news about Donald Trump just before last year's presidential election while straining to refocus criticism on the mainstream media and Hillary Clinton's campaign."¹¹⁰ The Associated Press' (AP's) wording, while more lyrical, was in line with what the U.S. intelligence community's assessment and the subsequent Senate Intelligence Committee reports.¹¹¹ As part of their analysis, the AP examined 36,210 tweets from August 31, 2015, to November 10, 2016. These tweets had been posted by 382 Russian accounts that Twitter had shared with congressional investigators in early November 2017. The following example shows one of the tweets examined by the AP, "MSM (the mainstream media) is at it again with Billy Bush recording ... What about telling Americans how Hillary defended a rapist and later laughed at his victim?" This example was tweeted on October 7, 2016, by the account "America_1st," shortly after *The Washington Post* released a

¹⁰⁸ Digital Forensic Research Lab.

¹⁰⁹ Samantha Korta, "Fake News Conspiracy Theories and Lies: An Information Laundering Model for Homeland Security" (master's thesis, Naval Postgraduate School, 2018), 109.

¹¹⁰ Ryan Nakashima and Barbara Ortutay, "AP Exclusive: Russia Twitter Trolls Deflected Trump Bad News," *Associated Press*, November 9, 2017, <https://apnews.com/fc9ab2b0bbc34f11bc10714100318ae1>.

¹¹¹ Senate Select Committee on Intelligence, *The Intelligence Community Assessment*, 4–6.

news article citing Trump’s comments about lewd behavior with women he made to *Access Hollywood* host Bush.¹¹² The chart in Figure 48 was published in the AP article. It shows the coordination of Kremlin sanctioned tweets and its increased volume during particular points of the campaign cycle.

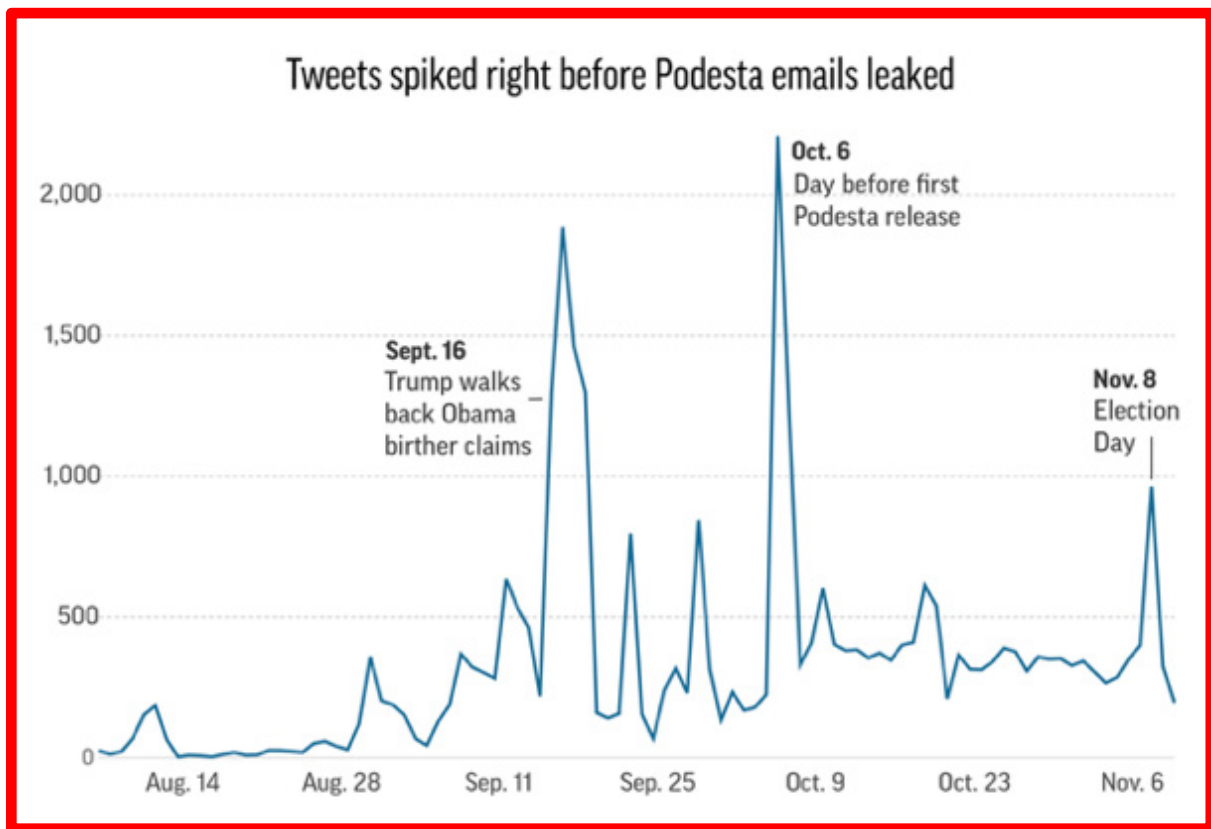


Figure 48. Associated Press Chart of Russian Twitter Traffic.¹¹³

The AP report examined how the Russian Twitter accounts had been presaging the WikiLeaks release of the Podesta email. “WikiLeaks’ Assange signals release of documents before U.S. election,” tweeted Kremlin accounts “SpecialAffair” and “ScreamyMonkey” within a second of each other on Oct. 4.”¹¹⁴ The AP also illustrated

¹¹² Nakashima and Ortutay, “AP Exclusive: Russia Twitter Trolls Deflected Trump Bad News.”

¹¹³ Source: Nakashima and Ortutay.

¹¹⁴ Nakashima and Ortutay.

how the account had been active earlier in the campaign, and noted, for example, high levels of activity when candidate Trump changed direction on his claims about President Barack Obama's birthplace by acknowledging it was the United States and not Kenya. Several Russian accounts spread the narrative that Hillary Clinton was actually responsible for the controversy around President Obama's birthplace, while others continued to propagate birther stories that stated the president was not native born. "TEN_GOP," a Russian account cleverly designed to appear as representative of the Tennessee Republican Party, posted a link stating that President Obama "admits he was born in Kenya."¹¹⁵ Further examples of Russian messaging attacking the Clinton campaign focused on the former Secretary of State's health. The "TEN_GOP" post in Figure 49, while from 2017, shows the continued amplification of Secretary Clinton's health problems.

¹¹⁵ Nakashima and Ortutay.



Figure 49. Content from the Russian Twitter Account “TEN GOP.”¹¹⁶

Notably, in a show of understanding for American culture, when Clinton returned to public campaigning after battling pneumonia in mid-September 2016, the Russian account “Pamela_Moore13,” started using the song *I Feel Good* by James Brown as background music, which it followed with text stating, “James Brown died of pneumonia.”¹¹⁷ This theme around Secretary Clinton’s fragile health was distributed by many other Kremlin-linked accounts.

Research based out of MIT’s Initiative on the Digital Economy released in March 2018, highlights why the Kremlin’s propaganda machine may have been so effective on social media. Among conclusions reached by the MIT research team was that false news was 70% more likely to be retweeted than true information. Furthermore, the MIT study

¹¹⁶ Source: UsHadrans, “Repository for Content from the Russian Social Media Account TEN GOP.”

¹¹⁷ Nakashima and Ortutay, “AP Exclusive: Russia Twitter Trolls Deflected Trump Bad News.”

showed that the false information spread faster and deeper than truth. The MIT analysis also stated that because humans retweeted false information and not automated bots, combating this problem would need to include solutions aimed at changing behavior.¹¹⁸

D. TARGETING VULNERABILITIES WITH AMPLIFIED AUTHENTIC CONTENT

In addition to the evident divisive nature of the propagandistic content, data sets are available to back up the intentions of the automated bots to drive a socially divisive agenda, in particular in more volatile population centers. Jonathan Albright of the Columbia University Tow Center has done significant analysis of Russian social media accounts during the 2016 election. In February 2018, he published an article in conjunction with Harvard's Berkman Klein Center that noted how troll accounts used by the Kremlin amplified genuine news coverage in U.S. cities suffering with racial, class, and other social divides. Cities targeted included, Chicago, Houston, St. Louis, Kansas City, Baton Rouge, and New Orleans.¹¹⁹ By using real news coverage and then amplifying the messages, the propagandist gained authenticity while still achieving their goal of pushing divisive narratives. The strategy which directly ties back to the overall goal of active measures, used real news coverage, often times from local news outlets, to set agendas for additional coverage in the Kremlin's interest, which pushed other journalist and influential members of the targeted communities to follow the stories.¹²⁰ The chart in Figure 50, published by Albright, shows where the fallacious Russian social media accounts sourced the genuine content it sought to amplify, while the chart in Figure 51, expresses the activity of 388 troll accounts during the covered time frame. The active web version of the data permits the display of all the account names, as well as their position on the chart at any given time.¹²¹

¹¹⁸ Sorous Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–1151, <http://science.sciencemag.org/content/359/6380/1146>.

¹¹⁹ Jonathan Albright, "Trolls on Twitter: How Mainstream and Local News Outlets Were Used to Drive a Polarized News Agenda," Harvard University, February 15, 2018, <https://medium.com/berkman-klein-center/trolls-on-twitter-how-mainstream-and-local-news-outlets-were-used-to-drive-a-polarized-news-agenda-e8b514e4a37a>.

¹²⁰ Albright.

¹²¹ Albright.

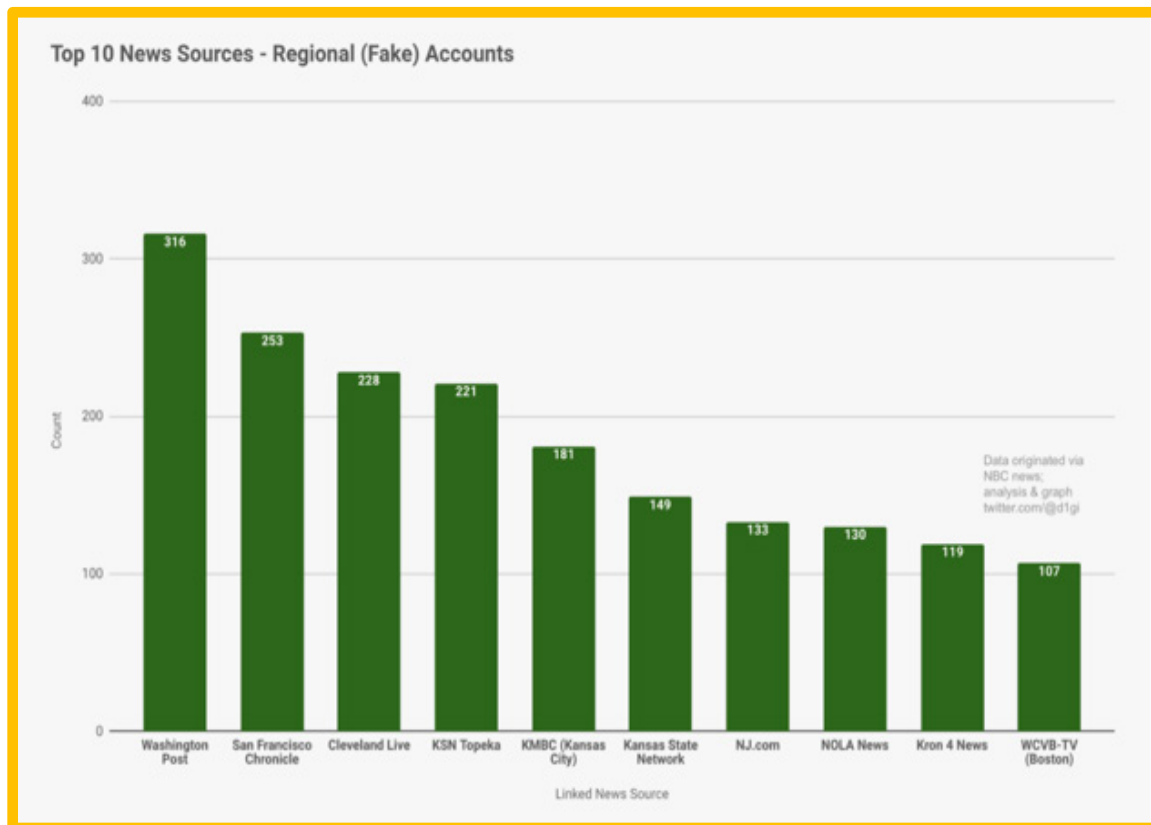


Figure 50. Berkman-Klein Chart of Media Sources Amplified by Russia's Propagandists.¹²²

¹²² Source: Albright.

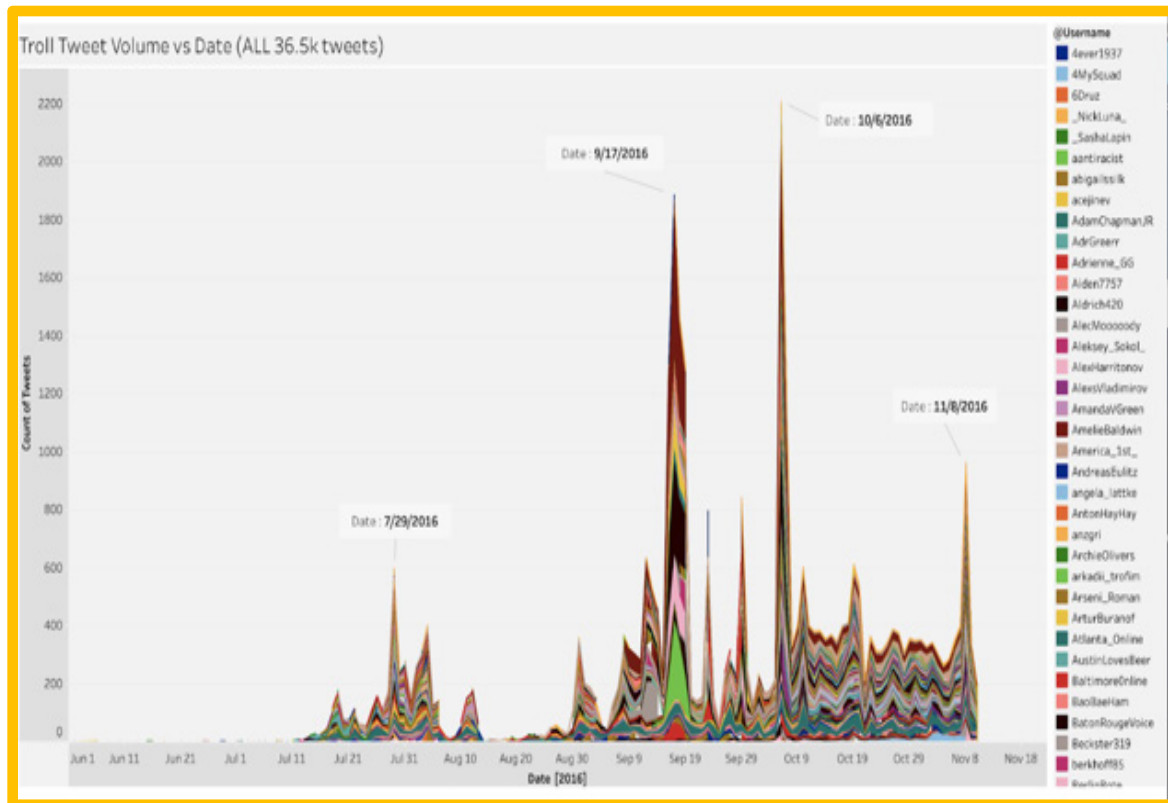


Figure 51. Berkman-Klein Chart of Russian Troll Twitter Account Activity.¹²³

Even with the most malicious and divisive social media posts that came out of the Internet Research Agency during the run up to the 2016 Presidential election, the Kremlin did not create the divided political terrain or the issues that strain social discourse in the United States. What Moscow achieved was an amplification of pre-existing stress points in American culture, in an attempt to increase political polarization and social discontent. Moscow's bots and trolls spread divisive messages on issues like race, immigration, religion, gay rights, gun control and more; however, these issues were already contentious subjects among the American people. Moscow's larger goal with the 2016 attack was not merely to wreak havoc with an election but to wreak havoc with a society by degrading public discourse and faith in the institutions of democracy. The goal in

¹²³ Source: Albright; "Troll Tweet Volume vs Date (ALL 36.5k Tweets)," Tableau Public, 2016, https://public.tableau.com/shared/SNHTMKBR?display_count=yes&:showVizHome=no.

other words, was to weaken the United States fundamentally as a nation, which is consistent with Moscow's ongoing information warfare strategy.

E. A CONCLUSION: WELL-REASONED DECEPTION THROUGH AMPLIFIED NARRATIVES

A review of the how Russia exploited the social media environment in 2016 shows the depth of understanding the Kremlin's propaganda agents had for both the psychology of human manipulation and the technology needed to implement it on a grand scale. To be sure, the Internet Research Agency did not invent misinformation and was not the first organization to use logical fallacies to gain a strategic advantage. Nation states throughout history, to include the United States, have attempted the propagandistic influence of adversary populations for their own interests. However, what Russia achieved in the 2016 attack was a prolific exploitation of cyberspace in this endeavor. In a masterful show of its understanding of influence operations, as well as information flow on the internet, Russia amplified media content both true and false. It did so while driving narratives designed to advantage the Russian Federation while weakening the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. THE RESPONSE TO THE KREMLIN ATTACK

A. THE U.S. GOVERNMENT: PROTEST, PUNISHMENT, AND CONGRESS LEARNS THAT SOCIAL MEDIA COMPANIES SELL ADVERTISING

Starting in late 2016, the United States' government began to respond publicly to the Kremlin's active measures campaign. This response took the form of sanctions, diplomatic expulsions, diplomatic protest, and the start of legal actions. On December 29, 2016, President Barak Obama announced, among other measures, the expulsion of 35 Russian intelligence operatives under diplomatic cover and the closure of Russian government compounds in Maryland and New York. President Obama further unveiled sanctions against nine entities and individuals associated with Russian intelligence services, while the U.S. Treasury Department identified two Russian individuals for cybercrimes related the 2016 election, to include theft of funds and personal information. The initial response set the template for the U.S. government's public response to the 2016 election attack.

To understand what the Russians had attempted and achieved during the run up to the 2016 election, the U.S. Congress held multiple hearings. Some of these hearings were public while others were held outside the public eye to protect national security related information. The subjects ranged from active measures to social media's role in dispersing propaganda. During some of the most publicized hearings, executives from social media companies, such as Facebook, Twitter, YouTube, and Google, were questioned about how their platforms had been exploited. Hearings held in fall 2017 revealed both how little Congress knew about the functioning of the social media industry, as well as Russia's ability to distribute propaganda over the internet. During these hearings, Facebook admitted that 126 million Americans may have been exposed to Russian propaganda on its platform and Twitter acknowledged that Russian accounts had

produced 1.4 million Tweets that generated 288 million impressions.¹²⁴ Congress' examination of Russia's role in the 2016 election continued through 2017 and 2018.

A 2018 House Intelligence Committee report stated, "In mid-February 2018, the Department of Justice charged 12 Russians and the Russia-based Internet Research Agency LLC with interference operations targeting the United States political and electoral processes... the stated goal of the Russian actors was to spread distrust towards the candidates and the political system in general." The House report noted the methods used by the Internet Research Agency included the use of stolen identities to establish false online personas, travel to the United States by operatives for collecting intelligence, and the way computer infrastructure was used to hide the Russian origin of the operation.¹²⁵

The U.S. Department of Justice has also been active in bringing legal action against Russian entities for the 2016 attack and other ongoing active measures campaign targeting Americans. On February 16, 2018, a federal criminal complaint was filed in the U.S. District Court for the District of Columbia. It targeted the Saint Petersburg-based Internet Research Agency and several of its Russian citizen employees for prosecution. The complaint stated:

From in or around 2014 to the present, Defendants knowingly and intentionally conspired with each other and with persons known and unknown to the Grand Jury to defraud the United States by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016.¹²⁶

¹²⁴ Dylan Byers, "Facebook Estimates 126 Million People Were Served Content from Russia-Linked Pages," CNN, October 31, 2017, <https://money.cnn.com/2017/10/30/media/russia-facebook-126-million-users/index.html?iid=EL>.

¹²⁵ U.S. Congress, House, *Report on Russian Active Measures* (Washington, DC: House Permanent Select Committee on Intelligence, 2018), 55, <https://permanent.access.gpo.gov/gpo91495/HRPT-115-1.pdf>.

¹²⁶ *United States v. Internet Research Agency*, Case 1:18-cr-00032-DLF Document 1 (U.S. District Court for the District of Columbia, 2018), 4–5, <https://www.justice.gov/file/1035477/download>.

While this charging document focused on activities related to the 2016 presidential election, it also revealed ongoing Internet Research Agency activity continuing into 2017.¹²⁷

In April 2018, an article in *Bloomberg News* noted a minimal amount of progress by the federal government in combating strategic weapons of influence over social media, and pointed to actions being taken by state governments.¹²⁸ It noted that California, with its high number of technology companies, was moving social media regulation forward. One piece of legislation listed was from California State Assemblyman Marc Levine, who has introduced a bill requiring the branding of bots with a disclaimer, while linking automated accounts and social media advertising purchases to verified humans. Similarly, in New York, the Governor and state assembly are working on legislation to require election advertising purchasers be identified on social media as with other mediums.¹²⁹

However, in late February 2019, it was widely reported that the U.S. Cyber Command was able to take the Internet Research Agency offline on November 6, 2018, the day of the U.S. midterm elections.¹³⁰ While no data points were available at the time this thesis was written about the efficacy of the Cyber Commands' efforts, this type of technological response to influence operations needs to be acknowledged as another tool in the counter information warfare toolbox. Nevertheless, it should not be viewed as a panacea. As has been noted by multiple sources, taking down this notorious producer of propaganda for a few days was likely intended to send a message to Russia about U.S. capabilities and resolve. If as reported, this operation only disabled the Internet Research Agency on Election Day. It could have done little to prevent its nefarious content from penetrating the subconscious minds of those Americans who had been viewing it for

¹²⁷ *United States*.

¹²⁸ Selina Wang, "California Would Require Twitter, Facebook to Disclose Bots," *Bloomberg*, April 3, 2018, <https://www.bloomberg.com/news/articles/2018-04-03/california-would-require-twitter-facebook-to-disclose-bots>.

¹²⁹ Wang.

¹³⁰ Jaqueline Thomsen, "US Cyber Operation Blocked Internet for Russian Troll Farm on Election Day 2018," *The Hill*, February 26, 2019, <https://thehill.com/policy/cybersecurity/431614-us-cyber-operation-blocked-internet-for-russian-troll-farm-on-election>.

months. As such, its impact on blunting strategic influence on the 2018 election was important but limited in scope.

B. TWO-FACEBOOK

Corporate America, in particular the social media industry, was slower to respond to the Russian internet threat. Of note, Facebook, which initially denied its platform had been exploited by Moscow's bots, trolls, and sock puppets, has since taken a much more aggressive posture in taking down hostile propaganda. As it became evident that the U.S. Congress was looking at regulatory possibilities for the social media industry, Facebook in fall 2017, ahead of the specter of public testimony about its role in the 2016 Russian attack, announced changes to its platform to prevent future exploitation.¹³¹

While Facebook was stepping up its cyber security resources and its monitoring of fallacious content on its platform, it was also waging its own social media propaganda operation. Facebook hired Definers Public Relations, a firm that engaged in tactics to protect Facebook's image, which its client had vowed to combat. Among these tactics, according to a report released by the *New York Times*, was the spreading of conspiracy theories over social media.¹³² One particular influence campaign organized by Definers for Facebook sought to paint technology companies Apple and Google in a negative light. This apparent retaliation resulted from the tech giants' criticism aimed at Facebook's ineffective privacy policy, as well as the Russian exploitation of the platform in 2016.

The alleged Facebook misinformation operation was described in this manner by the *New York Times*, "On a conservative news site called the NTK Network, dozens of articles blasted Google and Apple for unsavory business practices. One story called Mr. Cook (Apple CEO) hypocritical for chiding Facebook over privacy, noting that Apple also collects reams of data from users. Another played down the impact of the Russians' use of Facebook."¹³³ NTK is a Definers affiliate that uses content produced both by the

¹³¹ Frier, "Facebook Says it Will Double Safety and Security Staff to 20,000."

¹³² Sheera Frenkel et al., "Delay, Deny and Deflect: How Facebook's Leaders Fought through Crisis," *New York Times*, November 14, 2018, <https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html>.

¹³³ Frenkel et al.

latter, as well as America Rising, its opposition-research component. Though known for not having a large audience of its own, the NTK Network's content is frequently distributed by conservative outlets like Breitbart.¹³⁴ On November 15, 2018, after the *Times* published the story linking Definers and the social media company, Facebook without providing a reason, stated it had ended its relationship with the public relations firm.¹³⁵ The news of Facebook employing nefarious tactics to defend its own image while damaging that of its critics prompted the Nieman Lab at Harvard University to publish a synopsis of the *New York Times* story on its website under a banner stating, "Facebook probably didn't want to be denying it paid people to create fake news this week, but here we are."¹³⁶ An important takeaway from Facebook's clandestine and dishonest public relations efforts, is the cynicism it generated about the company's sincerity to combat nefarious activity on its platform. At a time when Facebook could have been completely transparent with the public, it was instead covering up its role in the 2016 election with disinformation.

Regardless of the conflictive message provided by Facebook's public testimony and covert propaganda campaign, the platform has made several announced security improvements since 2016. In January 2019, Facebook listed on its corporate news page an article entitled "Expanding our Efforts to Protect Elections in 2019."¹³⁷ While the article did not specifically mention Russia or the Internet Research Agency, the self-described approach Facebook is now employing appears designed to address Russia's tactics among others. Facebook stated it is addressing the problem with multifaceted countermeasures to include, "blocking and removing fake accounts; finding and removing bad actors; limiting the spread of false news and misinformation; and bringing

¹³⁴ Frenkel et al.

¹³⁵ Frenkel et al.

¹³⁶ Laura Hazard Owen, "Facebook Probably Didn't Want to be Denying it Paid People to Create Fake News this Week, But Here We Are," NiemanLab, November 16, 2018, <http://www.niemanlab.org/2018/11/facebook-probably-didnt-want-to-be-denying-it-paid-people-to-create-fake-news-this-week-but-here-we-are/>.

¹³⁷ Katie Harbath and Samidh Chakrabarti, "Expanding Our Efforts to Protect Elections in 2019," Facebook Newsroom, January 28, 2019, <https://newsroom.fb.com/news/2019/01/elections-2019/>.

unprecedented transparency to political advertising.”¹³⁸ According to this same article, Facebook, as of January 2019, employees 30,000 platform safety and security workers, which is three times more than it employed in 2017 for the same functions. Among the activities targeted by Facebook’s security personnel is “coordinated inauthentic behavior.”¹³⁹

C. TWITTER

In testimony provided to Congress in September 2018, Twitter CEO Jack Dorsey stated that the platform had identified 50,258 automated accounts linked to Russia during the 10 weeks prior to the 2016 election.¹⁴⁰ Dorsey also stated that Twitter had continued to identify and take down accounts linked to the Internet Research Agency, which he totaled as 3,843 accounts as of his September 2018 testimony. He specifically noted 18 accounts identified in March 2018, which he stated, “were created and registered after the 2016 election. These accounts used false identities purporting to be Americans, and created personas focused on divisive social and political issues.”¹⁴¹ While this number of accounts related to the total Twitter activity during the same time frame is very small, it does show the companies’ capability in identifying and mitigating hostile content, as well as its dedication to do the same.

D. INVESTIGATIONS LAUNCHED, CRIMINALS CHARGED, REGULATIONS PROPOSED, AND TECH GIANTS ADAPT

Looking back at the responses from the various sectors involved in countering Russia’s strategic weapons of influence, it is evident that all were playing catch up in understanding what the Kremlin had accomplished. Not that Russia’s information warfare strategy was a secret, as these tactics had played out to differing degrees in other nations. Nevertheless, the U.S. Congress initially seemed caught off guard by how this

¹³⁸ Harbath and Chakrabarti.

¹³⁹ Harbath and Chakrabarti.

¹⁴⁰ United States House Committee on Energy and Commerce, *Testimony of Jack Dorsey Chief Executive of Twitter* (Washington, DC: U.S. House of Representatives, 2018), 8, <https://docs.house.gov/meetings/IF/IF00/20180905/108642/HHRG-115-IF00-Wstate-DorseyJ-20180905.pdf>.

¹⁴¹ United States House Committee on Energy and Commerce, 10.

attack could have happened, and at the time, this thesis was written, had yet to pass any significant legislation to prevent this type of social media exploitation in the future. Yet, many congressional hearings were held in multiple committees to investigate the 2016 attack. The U.S. Department of Justice set about prosecuting criminals when it could (not easy when the bad actors are overseas), while the intelligence community continued to gather evidence and diplomats protested. The big social media companies? Facebook's denial and obfuscation about platform exploitation eventually evolved into public cooperation, with a significant ramp up in cyber security personnel. Twitter too has taken significant measures to monitor and self-regulate content on its platform. However, neither companies' actions were proactive but rather appear as a response to congressional, news media, and shareholder scrutiny.

THIS PAGE INTENTIONALLY LEFT BLANK

V. IMPACT OF RESPONSE

A. THE KREMLIN'S PERSISTENCE

From the time U.S. intelligence community attributed the election attack to Moscow in 2016 through late 2018, the official position by the Russian government has been to deny that it mounted an active measures campaign. Furthermore, at the highest levels of the U.S. government, there has been a disjointed political posture regarding Moscow's attempts to interfere with the election. Significant evidence shows that Moscow's attempts to influence U.S. political discourse have not stopped. The propaganda-tracking website Hamilton 68 continues to track automated propaganda emanating from Russian government linked organizations. Additionally, the Atlantic Council's Digital Forensic Research Lab documented Internet Research Agency propaganda traffic ahead of the 2018 midterm elections. In an article published on its website, it noted that Facebook took down 99 Instagram accounts, 36 Facebook accounts, and six Facebook pages for "coordinated inauthentic behavior," just prior to the 2018 election.¹⁴²

The impact of the U.S. government's response to curtailing the Kremlin's social media assault was minimal through 2017. Russia's strategic weapons of influence actually increased in number into late 2017. The chart in Figure 52 shows Internet Research Agency Twitter activity identified by the Oxford University's Computational Propaganda Project, as requested by the Senate Select Committee on Intelligence.¹⁴³

¹⁴² Ben Nimmo et al., "#TrollTracker: Facebook's Midterm Takedown, Analyzing the Accounts Attributed to Russia's Internet Research Agency," Digital Forensic Research Lab, November 13, 2018, <https://medium.com/dfirlab/trolltracker-facebooks-midterm-takedown-f3451ee5dc2>.

¹⁴³ Howard et al., *The IRA, Social Media*, 4–5.

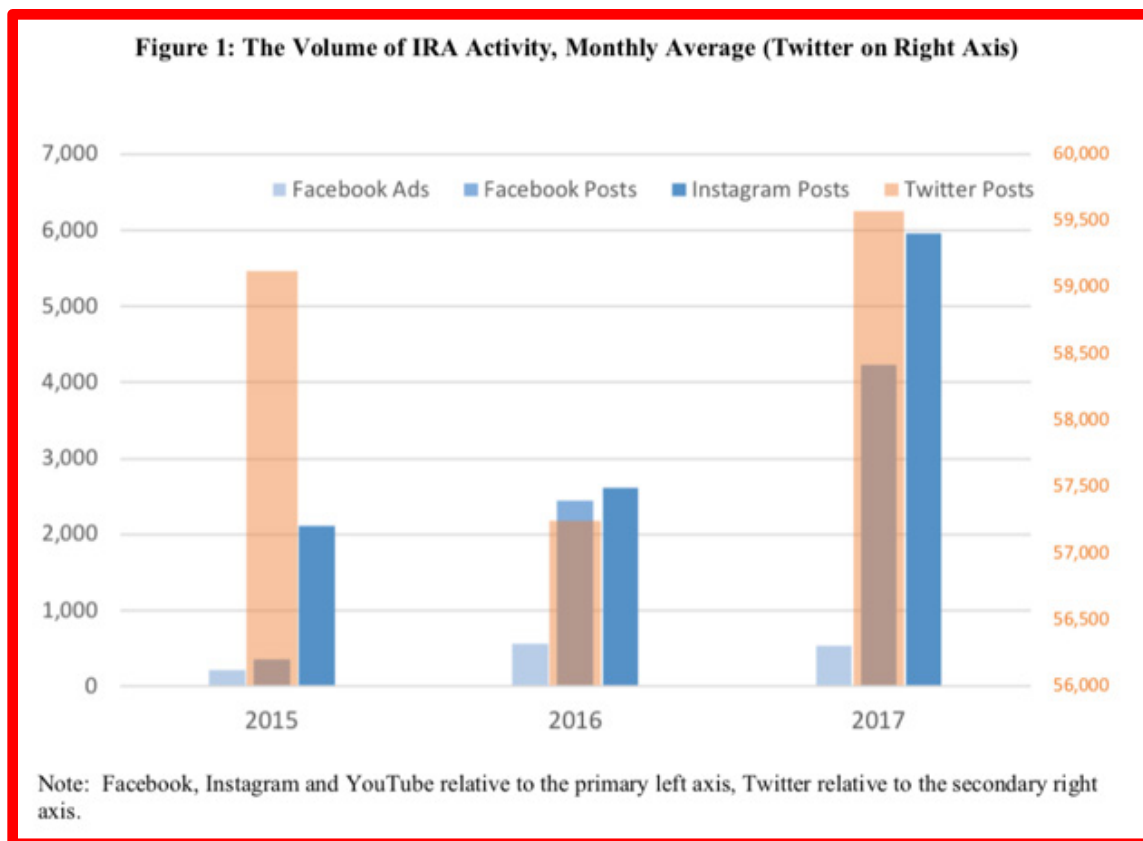


Figure 52. Internet Research Agency Twitter Activity as Compiled by the Computational Propaganda Project.¹⁴⁴

B. JUSTICE FINDS EVIDENCE, “PROJECT LAKHTA”

Beyond the evidence of active measures still being uncovered by nongovernmental organizations, academia, and social media companies, the U.S. Department of Justice continues legal action against Russian government officials related to these attacks. In late September 2018, the United States Attorney for the Eastern District of Virginia filed charges against a Russian woman working with the Internet Research Agency for attempts to interfere in the 2018 U.S. midterm elections. The tactics described in the filing document were similar to those listed by the DNI in the 2017

¹⁴⁴ Source: Howard et al., 5.

report on Russian activity during the 2016 election that included deploying divisive propaganda over social media to sow discord amongst the American people.¹⁴⁵

Further evidence states that the Kremlin's bots and trolls were active in trying to influence the 2018 U.S. midterm elections. On September 28, 2018, a federal criminal complaint was filed against a Russian woman named Elena Alekseevna Khushyaynova in the Eastern District of Virginia. The complaint alleges that Khushyaynova, connected to the Internet Research Agency, and "Project Lakhta," conducted an ongoing conspiracy to mount influence operations against the United States on behalf of the Kremlin.¹⁴⁶ The 38-page complaint contained an in detail description of the structure, goals, and methods including several examples of social media propaganda produced by this ongoing active measures operation. The following passages are quoted directly from the complaint:

The Conspiracy had as its objects impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable Project Lakhta actors to interfere with US. political and electoral processes, including the 2018 US. elections.

The Conspiracy has a strategic goal, which continues to this day, to sow division and discord in the US. political system, including by creating social and political polarization, undermining faith in democratic institutions, and influencing US. elections, including the upcoming 2018 midterm election. The Conspiracy has sought to conduct what it called internally, information warfare against the United States of America through fictitious U.S. personas on social media platforms and other Internet-based media.

Between in or around December 2016 and in or around May 2018, as part of the Conspiracy's effort to sow discord in the US political system, members of the Conspiracy used social media and other Internet platforms to inflame passions on a wide variety of topics, including immigration, gun control and the Second Amendment, the Confederate flag, race relations, LGBT issues, the Women's March, and the NFL national anthem debate. Members of the Conspiracy took advantage of specific events in the United States to anchor their themes, including the shootings of church members in Charleston, South Carolina, and concert attendees in

¹⁴⁵ *United States of America v. Elena Alekseevna Khushyaynova*, 1:18-MJ-464 (United States District Court for the Eastern District of Virginia, September 28, 2018), 6, <https://www.justice.gov/opa/press-release/file/1102316/download>.

¹⁴⁶ *Elena Alekseevna Khushyaynova*, 4–6.

Las Vegas, Nevada; the Charlottesville Unite the Right rally and associated Violence; police shootings of African-American men; as well as the personnel and policy decisions of the current US. administration.

Members of the Conspiracy were directed to create political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements.¹⁴⁷ The Conspiracy also sought, in the words of one member of the Conspiracy, to effectively aggravate the conflict between minorities and the rest of the population.¹⁴⁷

The criminal complaint continued with a description of the following specific targeted operations by Project Lakhta:

On or about December 10, 2017, a member of the Conspiracy used the Twitter account “@CovfefeNationUS” to repost a Tweet encouraging readers to donate to a political action committee aiming to unseat Democratic Senators and Representatives in the 2018 midterm election.

On or about February 8, 2018, a member of the Conspiracy used the Twitter account “@Amconvoice” to post a Tweet about the 2018 US. midterm election: The only way the Democrats can win 101 GOP seats is to cheat like they always do with illegals dead voters.

On or about February 19, 2018, a member of the Conspiracy used the Twitter account “@KaniJackson” to post a Tweet about the 2018 midterm election: Midterms are in 261 days, use this time to: Promote your candidate on social media Volunteer for a campaign Donate to a campaign Register to vote Help others to register to vote Spread the word We have only 261 days to guarantee survival of democracy. Get to work!

On or about May 17, 2018, a member of the Conspiracy used the Twitter account “@KaniJackson” to repost two Tweets about a US. Senate vote on Net Neutrality: Ted Cruz voted to repeal #NetNeutrality. Let’s save it and repeal him instead. Here’s the list of GOP senators who broke party lines and voted to save #NetNeutrality: Susan Collins John Kennedy Lisa Murkowski Thank you!¹⁴⁸

As in the attack on the presidential election, the Internet Research Agency from 2017 through 2018 exploited social media by driving narratives that were as inconsistent as they were corrosive, which shifted at times from supporting Republican candidates to supporting Democratic causes. Most telling from the court documents was the stated

¹⁴⁷ *Elena Alekseevna Khusyaynova*, 6–13.

¹⁴⁸ *Elena Alekseevna Khusyaynova*, 32–38.

Russian objective of using socially divisive propaganda in another attempt at eroding U.S. democratic processes.

C. TORMENT THE TORMENTOR

Adding to the evidence of ongoing Russian active measures contained in the Project Lakhta complaint, was a related Justice Department court document from January 2019.¹⁴⁹ It showed that Russia exploited the polarized political climate in the United States to discourage further consequences for its influence operations targeting the 2016 presidential election. In the filing, federal prosecutors identified a Russian strategic weapon of influence whose target was to undermine the investigation into Kremlin's active measures campaign against the 2016 presidential election. The court document identified the Russian Twitter account @HackingRedstone. It stated this account had released authentic but non-public legal discovery documents mixed with fallacious material. Accusing @HackingRedstone of portraying this mix of material as the total evidence law enforcement, in particular Special Counsel Robert Mueller, holds against Russia and the Internet Research Agency. The prosecution filing described it as "apparent effort to discredit the investigation."¹⁵⁰ While this influence weapon was much smaller in scale than the 2016 operation, it nevertheless followed a similar pattern of hacking, release of non-public documents, spurious content, and the goal of shifting public opinion in a direction beneficial to the Kremlin. The content in Figure 53 further exemplifies the Kremlin's efforts to discredit Special Counsel Robert Mueller while additionally painting Russia in a positive light.

¹⁴⁹ *United States v. Concord Management and Consulting LLC*, Case 1:18-cr-00032-DLF Document 94 (U.S. District Court for the District of Columbia, 2019), 1, <http://cdn.cnn.com/cnn/2019/images/01/30/2019-1-30concord.2.pdf>.

¹⁵⁰ *Concord Management and Consulting LLC*, 1.

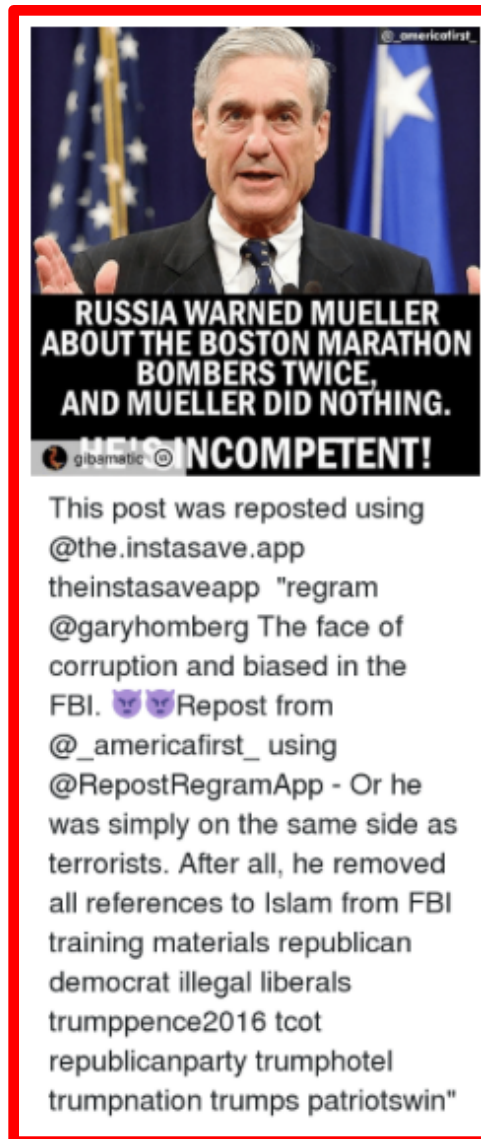


Figure 53. Content from the Russian Social Media Account “AmericaFirst.”¹⁵¹

D. DIGITAL FORENSIC LAB OBSERVATIONS/ MEDIUM AND HAMILTON 68

Two years downstream from its attempted interference in the 2016 U.S. presidential election, evidence shows beyond the federal criminal proceedings that the Kremlin directed Internet Research Agency is still seeking to influence social and

¹⁵¹ Source: UsHadrans, “This Space Is a Repository for Content from the Russian Social Media Account ‘_AmericaFirst_’.”

political discourse in the United States. Social media propaganda tracking organizations like the Atlantic Council's Digital Forensic Research Lab and the German Marshall Fund's Hamilton 68, continue to see coordinated campaigns. In November 2018, Facebook provided evidence documented by the Digital Forensic Research Lab. This evidence demonstrated that the Internet Research Agency's efforts were still bearing fruit. According to an article posted to the Lab's website on *Medium* from November 13, 2018, Facebook took down 99 Instagram, 36 Facebook accounts, and six Facebook pages for what it described as "coordinated inauthentic behavior," and stated around 1.25 million other users followed at least one of them.¹⁵² While neither the Digital Forensic Research Lab nor Facebook directly attributed the accounts or pages to the Internet Research Agency, they pointed in that direction. The Digital Forensic Research Lab article went on to describe these newly identified coordinated sites modus operandi and their links to past Internet Research Agency propaganda. As with prior Russian generated content, errors in syntax and grammar resembled some of the older St. Petersburg product. Of particular note was the omission or incorrect usage of grammatical articles that do not exist in Slavic languages. Figure 54 contains a few examples of these kinds or errors as they appeared in the stricken social media products listed by the Digital Forensic Research Lab.

¹⁵² Nimmo et al., "#TrollTracker: Facebook's Midterm Takedown."

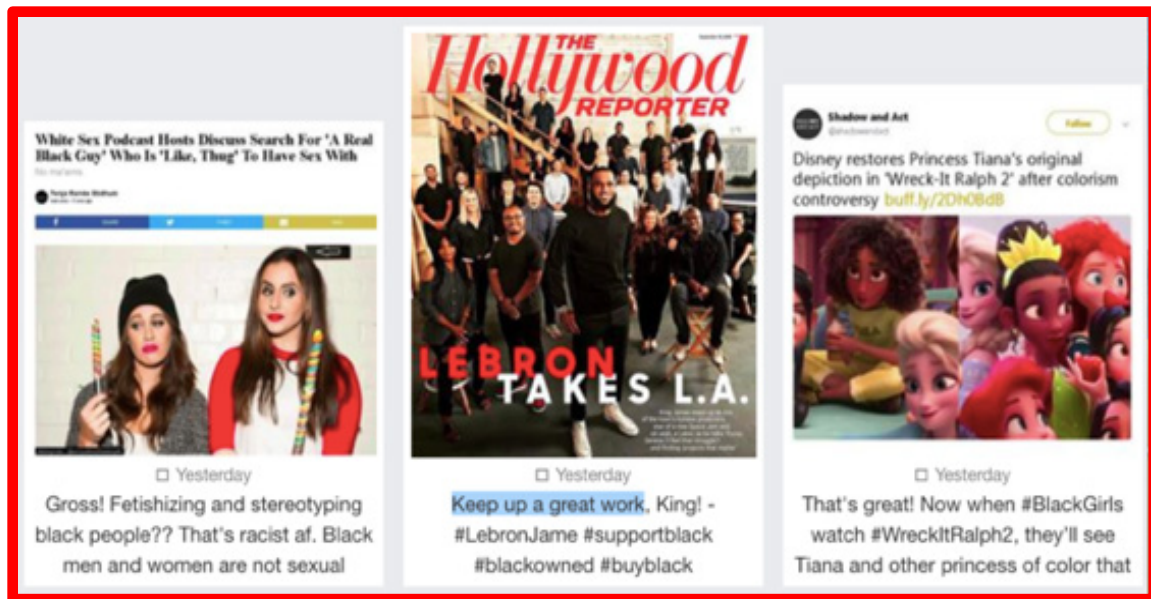


Figure 54. Digital Forensic Research Lab Compilation of Grammatical Errors in Russian Content.¹⁵³

Beyond the ubiquitous grammar and syntax errors common to Internet Research Agency propaganda, the Digital Forensic Research Lab noted other commonalities. For example, some of the newer content taken down by Facebook was actually older material that still carried watermarks from known Internet Research Agency products.¹⁵⁴ Figure 55 shows an example of watermarked content as posted on the lab's website.

¹⁵³ Source: Nimmo et al., “#TrollTracker: Facebook’s Midterm Takedown.”

¹⁵⁴ Nimmo et al.

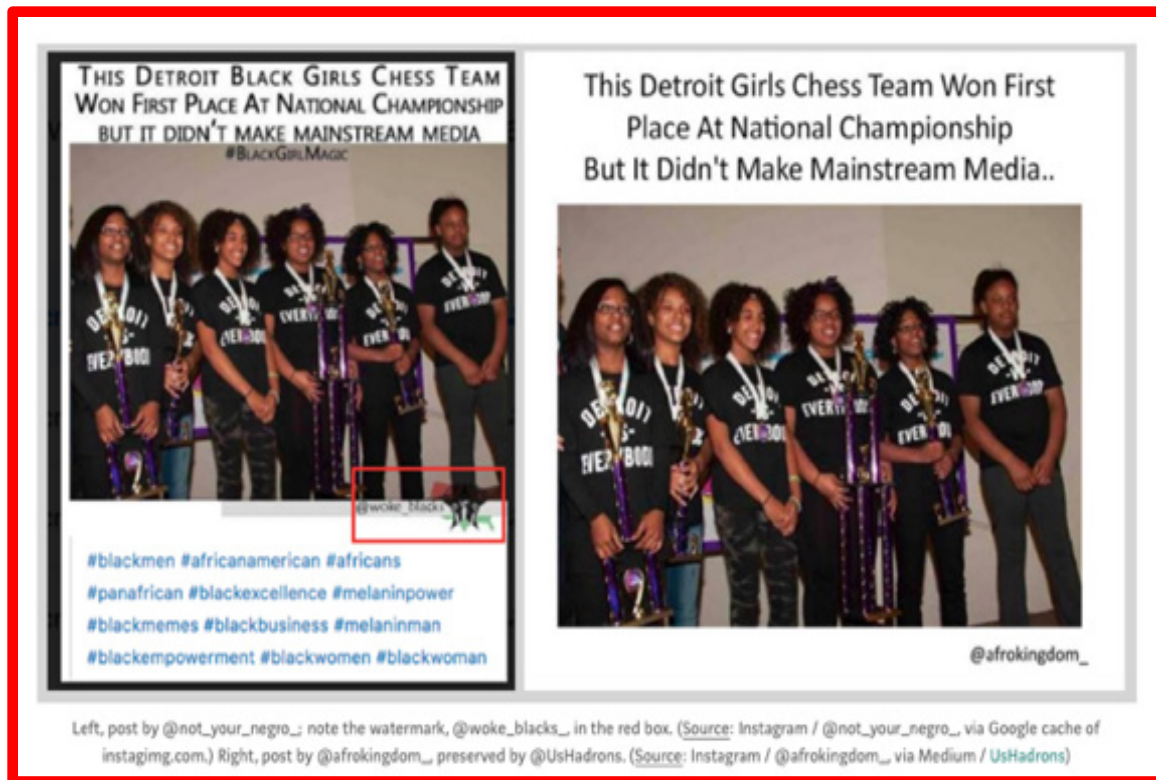


Figure 55. Digital Forensic Research Lab Image Showing Watermarks in Two Generations of Russian Content.¹⁵⁵

Once again, evidence of coordination can be seen between the social media propaganda efforts and messages being put out by Russian state news outlets. This coordination should not be surprising, as it is in line with classic Russian active measures doctrine. However, the Digital Forensic Research Lab article stated the following caveat: “Posting divisive content is not, again, sufficient to expose a Russian troll account; indeed, without American trolls, Russian trolls would have nobody to disguise themselves as. However, it is in character with earlier Russian troll operations.”¹⁵⁶ The Instagram post in Figure 56 included language that came directly from Russian state media outlet Sputnik but without attribution.

¹⁵⁵ Source: Nimmo et al.

¹⁵⁶ Nimmo et al.

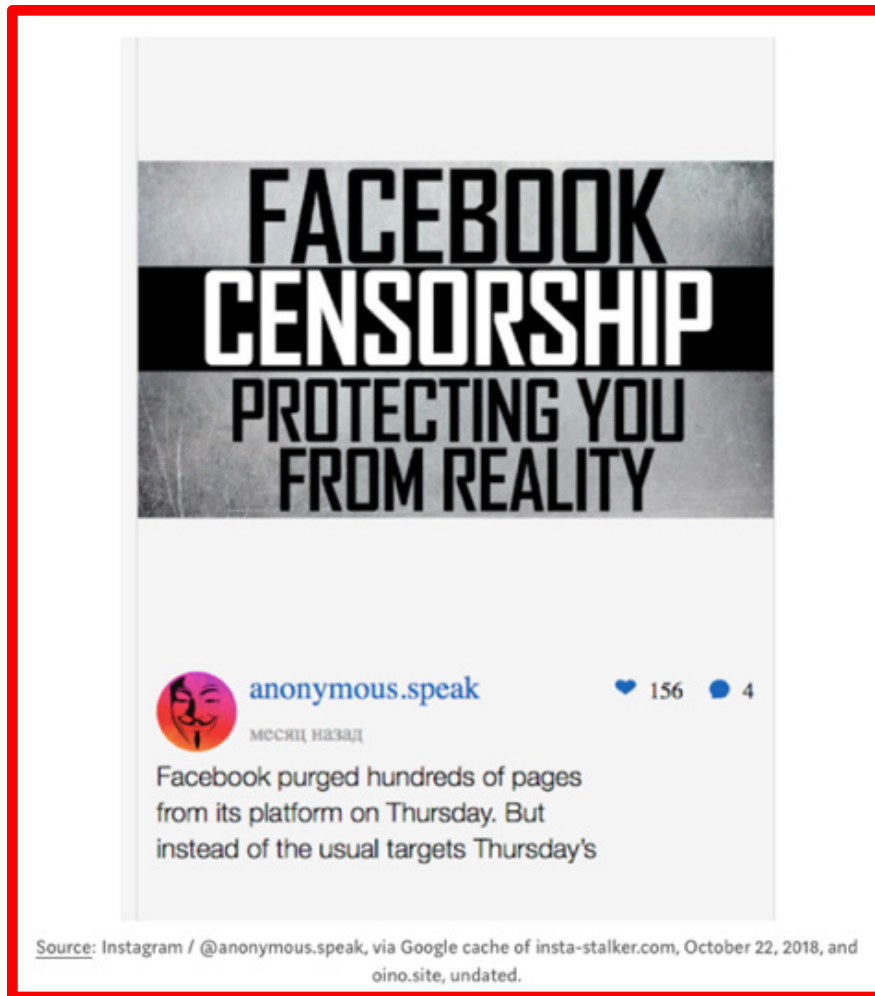


Figure 56. Digital Forensic Research Lab Image Sputnik Sourced Language on Fallacious Instagram Post.¹⁵⁷

While the Digital Forensic Research Lab noted the grammatical errors, Hamilton 68 pointed out in its November 2018 report that using these mistakes as evidence of a Russian operation was not accurate or statistically relevant. The Hamilton 68 report went further by noting that mistakes indicative of non-English speaking Russians were more the exception than the rule in the content it examined.¹⁵⁸ This viewpoint also makes sense as the propagandists have access to the same information as the general public and are able to learn from past mistakes. Furthermore, in that much of the active measures'

¹⁵⁷ Source: Nimmo et al.

¹⁵⁸ Schafer, "A View from the Digital Trenches."

material was simply reposted and amplified authentic content from other sources, relying on grammar and syntax to identify hostile posts would leave the majority of the material intact, circulating, unmonitored, and unchecked.

A separate Digital Forensic Research Lab's article concerning the 2018 midterm election pointed to both the progress made in tracking and taking down hostile content, but also acknowledged the challenge in alerting the targeted population. Its analysis credited cooperation between the U.S. law enforcement community and social media companies to responding to the threat but noted that inauthentic trolls are still operating to target divisions in American society. Nevertheless, while this improvement in defense by key organizations on the U.S. side leads to some degree of optimism, the challenge still remains for how to alert targeted populations about the threat.¹⁵⁹

Therefore, while sanctions, expulsions, and official protest by the U.S. government have made a show of displeasure with Moscow, they have not completely deterred or prevented ongoing active measures attacks by midyear 2018. Nor had the efforts in the private sector completely eliminated the exploitation of its platforms. The trolling taunt posted by the Kremlin's propagandists in Figure 57 hints at this adversary's resolve.

¹⁵⁹ Nimmo et al., "#TrollTracker: Facebook's Midterm Takedown."



Tag you bro... The Great Meme War is not over! Let's asseble here. americaneagle

Figure 57. Content from the Russian Social Media Account “Angry Eagle.”¹⁶⁰

¹⁶⁰ Source: UsHadrans, “This Space Is a Repository for Content from the Russian Social Media Account ‘Angry Eagle’.”

VI. OBSERVATION AND RECOMMENDATIONS FOR FUTURE POLICIES: TRANSPARENCY, EDUCATION, AND AWARENESS

A. COMBATING STRATEGIC WEAPONS OF INFLUENCE WILL REQUIRE POLITICAL UNITY AND PUBLIC AWARENESS

Much in the same manner that Osama Bin Laden underestimated the resiliency of the American people, Vladimir Putin has underestimated America's structural strengths, including freedom and democracy. It is possible that once the political controversies surrounding the 2016 election have run their course, that the American people will shrug off the Kremlin's active measures as a mere nuisance of little importance.

The difference of course between 9/11 and the Kremlin's assault on the 2016 election is that the prior attacks galvanized the American people into action to combat a common enemy. The same cannot be said for the 2016 attack on the U.S. democracy, which continues to divide the American public along political and ideological lines. However, that of course was the point! The value of these operations in late 2018 might be best gauged by the Kremlin's persistence in the face of diplomatic protests, legal penalties, and international condemnation. The Kremlin's continued deployment of strategic weapons of influence over social media could be the best evidence available for Russia's belief in their effectiveness. It is also the best proof for why the United States needs a coherent counter strategy, including a plan to build awareness about the threat.

B. RAISE THE COST, AND FOLLOW OUR OWN ADVICE

If the price for this kind of attack was possibly made higher, Russian leaders might change their tactics.¹⁶¹ In March 2018, a U.S. House of Representatives Permanent Select Committee on Intelligence report stated:

The effectiveness and relatively low cost of information operations, such as the dissemination of propaganda, make it an attractive tool for foreign adversaries. Unless the cost-benefit equation of such operations changes

¹⁶¹ U.S. Congress, House. *Report on Russian Active Measures*, 3.

significantly, the Putin regime and other hostile governments will continue to pursue these attacks against the United States and its allies.¹⁶²

This same Congressional document makes several recommendations on Russian active measures operations in both Europe and the United States.

The House Intelligence Committee also noted the following about the tactics against European targets, “Russia targets disaffected European populations and exploits social, political, and racial divisions in an effort to sow discord, encourage unrest, and incite protests.”¹⁶³ The report makes no such claim about similar tactics in the United States. This omission is interesting in light of the nature of Russian propaganda targeting the United States. It has been widely acknowledged in popular media, intelligence reports, and in testimony by social media executives before the U.S. Congress, that the Russian propaganda targeting the American people was socially divisive. Nevertheless, the House Intelligence report did make recommendations for European countermeasures that could be applicable in the United States including the following:

#1: European governments, non-governmental organizations, businesses, think tanks, and academia should strengthen legal and regulatory environments, promote media pluralism, build professional media associations, and improve the financial sustainability of legitimate news outlets. #2: European governments, non-governmental organizations, businesses, think tanks and academia should implement and encourage multi-pronged, country-wide efforts by both public and private entities to combat Russian propaganda, technical, and cyber operations... Russia utilizes a whole-of-government approach in its information operations, mobilizing a variety of tools to achieve its goals. From hacking of government networks, think tanks, and universities to spreading propaganda via social media, Russia’s tentacles are many and far reaching... It is therefore imperative that Western nations implement countrywide efforts to educate its populations and inoculate their governments, media outlets, and other organizations from Russian influence campaigns. To do this, Western nations should encourage increased partnership between public and private entities in order to combat Russian information, technical, and cyber operations.¹⁶⁴

¹⁶² U.S. Congress, House, *Report on Russian Active Measures*, 3.

¹⁶³ U.S. Congress, House, 15.

¹⁶⁴ U.S. Congress, House, 114.

From the aforementioned congressional recommendations for Europe, a couple particular standouts for the United States should be mentioned. The first is to educate Americans about the threat, providing an inoculative effect for future influence attacks. The second is to encourage countrywide cooperation among various organization from the government, private sector, and academia. Just as launching this kind of attack requires divergent talents from technological prowess to psychosocial understanding, the strategy to combat this threat must also tap a wide variety of assets while engaging multiple sectors of society. The United States is the global leader in information technology and has an enviable higher education system full of world-class research universities like the Naval Postgraduate School. Furthermore, the U.S. constitution and the democratic structures it created have endured for over 200 years with a self-evident degree of success. To engage all these strengths in combating a common enemy should require little debate.

C. BUILD ON THE PRESENT

Building on the proceeding recommendations, legislatures should keep the measures in place that have been implemented since 2016 to counter the Kremlin's actions. The U.S. government needs to keep investigating the nefarious actors targeting the American people with strategic weapons of influence. The U.S. Department of Justice should continue to prosecute individuals and organizations committing criminal acts under U.S. law in furtherance of their propaganda goals. Diplomatic pressure should be increased against the Russian government to curtail deploying these information warfare weapons, while U.S. cyber forces continue to work their dark magic.

Internally, U.S. legislators need to continue to scrutinize the behavior of social media companies and encourage them to track and take down hostile foreign content (not to be confused with First Amendment protected offensive content). This removal can be accomplished with ongoing industry oversight, to include more congressional hearings should social media platforms revert to policies that permit the distribution of hostile propaganda. Congress could also pass a version of the Honest Ads Act to increase transparency for politically funded activity on the internet.

The aforementioned measures should be the base of a larger coherent strategy to combat influence operations. An important piece of this strategy will be investing in developing the cognitive ability in the American people to resist influence weapons, whether deployed over today's social media or through whatever new communication technology may emerge. An important component to this strategy is to alert the population actively about the threat. In a democracy, the people are the ultimate policy decision makers; therefore, they need to know when a foreign power is attempting to get them to conform to its interests. If people understand how this manipulation takes place and that they are being deliberately targeted by propaganda, they may become more discerning consumers of the information flows that wash over them on a daily basis.

Claire Wardle put forward another approach to cognitive defense in her *First Draft* article. She advised content consumers to be more deliberate with how they view and share information and encourages them to be more skeptical. Wardle proposes that the impact of misleading information may be blunted but it will take some work, and she offers the following advice:

If you find yourself incredibly angry at a piece of content or feeling smug (because your viewpoint has been reaffirmed), take another look... In the same way that you're told to wait 20 minutes before you reach for a second helping of food, because you need to wait for your brain to catch up with your stomach, the same is true with information. Maybe you don't need to wait 20 minutes before clicking the share button, but two minutes is probably sensible.¹⁶⁵

Building intellectual resistance to propaganda also dovetails with U.S. national defense priorities. In his 2018 article for the Army War College, U.S. Navy Commander Timothy McGeehan noted how President Eisenhower used the National Defense Education Act to improve public education, especially in the areas of science and engineering to benefit national security. McGeehan stated that the same emphasis is needed today to use education to counter disinformation.¹⁶⁶

¹⁶⁵ Wardle, "Fake News: It's Complicated."

¹⁶⁶ Timothy McGeehan, *Countering Russian Disinformation* (Carlisle, PA: Army War College, 2018), 54, https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf.

In 2016, with evidence in hand that the Kremlin was waging a major campaign to influence the presidential election, neither the White House nor the U.S. Congress took substantial action to alert the American public. Retired Ambassador and U.S. NATO representative Nicholas Burns, as he testified before the U.S. Senate in June of 2017 stated:

With the benefit of hindsight, the Obama Administration should have reacted more quickly and vigorously last summer and autumn to respond to the Russian hacking of the Democratic National Committee and its effort to harm Secretary Hillary Clinton's campaign. It should have been much more transparent with the American public about what it knew and the threat it clearly posed to the election.¹⁶⁷

Reinforcing this sentiment about the importance of public transparency when confronting this type of threat, Janis Sarts, Director of the NATO Strategic Communications Center of Excellence, during his testimony to the U.S. Senate in 2017, made the point this way:

The influence operations [the] Kremlin is pursuing are based on old soviet techniques combined with [the] clever use of our technologies and increasingly of our marketing knowhow. I see no reason why we should be losing. It is about acknowledging the problem, resourcing solutions and using that is best in our societies (free speech, civic engagement, innovation) to win it for our future.¹⁶⁸

Building off Sart's testimony, Congress should support a study for ways to inform the public about active influence operations, taking into consideration not revealing sensitive intelligence techniques. Regardless of the type of alert system that policy makers choose, not to inform should no longer be an option. As the minds of the public are the targets, and can be harmed by the inevitable gaslighting that accompanies influence operations, not to warn can possibly be viewed as an abdication of governmental responsibility. Thus, research on best practices for notifying the public of emerging influence threats should be conducted and the experiences of other nations considered.

¹⁶⁷ *Testimony on Russian Interference in European Elections Senate Select Committee on Intelligence Ambassador (ret.) Nicholas Burns June 28, 2017*, Senate, 115th Cong., 1st sess., June 28, 2017, 4, <https://www.intelligence.senate.gov/sites/default/files/documents/sfr-nburns-062817b.pdf>.

¹⁶⁸ *Testimony on Russian Interference in European Elections*, 6.

D. ENGAGING THE WHOLE SOCIETY

An article published in the *Journal of Strategic Studies* referencing Sweden's experience with Russian active measures, examined what its authors, Martin Kragh and Sebastian Åsberg, described as the Kremlin's continued use of public diplomacy combined with active measures for strategic purposes.¹⁶⁹ This study focused on Moscow's efforts in Sweden and the greater Baltic region from 2014 to 2017, and in particular, Russia's messaging supporting an anti-NATO and EU agenda while justifying its actions in the Ukraine. While Kragh and Åsberg looked at contemporary Russian influence operations, they also examined tactics used during the Soviet period. The authors hypothesis that reemerging "behavioral patterns from the Cold War period," point towards a careful examination of this history.¹⁷⁰

Facing a constant Russian propaganda barrage, Sweden developed strategies for defending its population and institutions against malign influences. What has emerged from this experience is an approach that engages multiple sectors of society, or the "whole of society," in defending against the negative impact to social discourse from this type of attack. This model includes involving the government, civil society, media, the private sector, and educational institutions with an emphasis placed on teaching critical thinking along with media literacy.¹⁷¹ The Swedish Civil Contingencies Agency (MSB), comparable in function to the U.S. Department of Homeland Security, listed the following information in a brochure distributed to all the nation's residents, "Be on the lookout for false information,—States and organizations are already using misleading information in order to try and influence our values and how we act. The aim may be to reduce our resilience and willingness to defend ourselves." The MSB brochure also recommends the critical appraisal of sources as the best protection against hostile

¹⁶⁹ Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 773–816, doi: 10.1080/01402390.2016.1273830.

¹⁷⁰ Kragh and Åsberg, 776.

¹⁷¹ Swedish Civil Contingencies Agency, *Important Information for the Population of Sweden: If Crisis or War Comes* (Karlstad: Swedish Civil Contingencies Agency, 2018), 6, <https://www.msb.se/en/>.

propaganda and advises the public to ask questions about information sources, their aims, and their credibility.¹⁷²

This “whole of society” approach was noted in a 2018 minority staff report prepared for the Committee on Foreign Relations in the U.S. Senate. The report entitled *Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, noted the Swedish efforts to resist Russian influence operations were being headed by the MSB, which was monitoring fake news stories pushing false narratives.¹⁷³

The focus on preparing the target audience for information warfare attacks has been noted as being particularly effective by other organizations. In Janis Sarts’ testimony to the U.S. Senate, his first recommendation for combating strategic weapons of influence through cyber space was raising society’s awareness. Sarts stated:

As has been described before, society and its perceptions are the main targets of the contemporary influence operations. Accordingly, one of the key resilience mechanisms, our research shows, is awareness of the society of being targeted by third party malicious actors... We have seen resilience levels raise instantly as society recognizes being targeted by outside actor.¹⁷⁴

In his testimony, Sarts emphasized the importance of educating targeted populations about the threat from influence operations.

It is not just a recommendation from national security experts, psychologists, or Nordic bureaucrats that the public should be educated about manipulation on social media. It is also the opinion of a once prolific hacker and producer of online propaganda. Andrés Sepúlveda, who plied the trade of social media manipulation in Latin America for several years in the interest of political campaigns, provided his insights in a March of

¹⁷² Swedish Civil Contingencies Agency, 6.

¹⁷³ Committee on Foreign Relations, *Putin’s Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security* (Washington, DC: United States Senate, 2018), 111, <https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf>.

¹⁷⁴ S., *Russian Intervention in European Elections*, 5.

2016 Spanish language interview with *Bloomberg News*.¹⁷⁵ Sepúlveda, who was in jail in Colombia for his activities at the time of the interview, even then believed nefarious forces were at work in the U.S. elections. His ability to see influence operations at work came from his experience in being the orchestrator as similar operation in multiple countries. Sepúlveda stated, “*Mi trabajo era hacer acciones de guerra sucia y operaciones psicológicas, propaganda negra, rumores, en fin, toda la parte oscura de la política que nadie sabe que existe pero que todos ven*” (“My work was that of a dirty war, psychological operations, black propaganda, rumors, in all, the shadowy parts of politics nobody knows exists, but that everyone gets to see”).¹⁷⁶ Apart from his interview with *Bloomberg News*, Sepúlveda had provided interviews to Colombian media outlets. In one of those interviews to *Enter* from April 2016, translated by Erin Gallagher on the website Medium, Sepúlveda stated the following about how to combat influence operations:

The first step to combating the problem of disinformation on social media is recognizing that—regardless of party or personal politics—we are all targets, we are all exposed to propaganda and susceptible to manipulation. But we can build up collective immunity to these kinds of operations by learning how to recognize social media manipulation and calling it out when we see it.¹⁷⁷

As such, this professional election manipulator not only provided a warning for what was taking place in the elections but also was presenting an education-centered roadmap for reducing the effects of strategic weapons of influence.

While certainly some policymakers in the United States understand the benefits to educating the population about the dangers presented by hostile foreign propaganda, no efforts had been made in this regard at the time this research was conducted, but it should change. Russia has once again asserted itself as a primary threat to U.S. homeland security. As the United States shifted focus from the Cold War paradigm of east vs. west

¹⁷⁵ Jordan Robertson, Michael Riley, and Andrew Willis, “Como hackear una eleccion,” *Bloomberg*, March 31, 2016, <https://www.bloomberg.com/features/2016-como-manipular-una-eleccion/>.

¹⁷⁶ Robertson, Riley and Willis.

¹⁷⁷ Erin Gallagher, “Fighting Disinformation on Social Media,” Medium, October 9, 2018, https://medium.com/@erin_gallagher/best-practices-on-social-media-for-midterm-elections-c821386d4ec0.

and became fully occupied with the Global War on Terror, Vladimir Putin set a course to reestablish Russia as the great power it was during the years of the Soviet Union. His government in Moscow identified cyberspace as an opportunity for deploying strategic weapons of influence. The Kremlin is using information warfare to weaken NATO aligned nations and the United States from the inside out by exploiting media outlets, as well as cyberspace, to divide society and promote social unrest. This same strategy played out in Russia's interference in the 2016 U.S. presidential election and continued right into 2018. Moscow's internet trolls, in coordination with traditional media outlets like RT, spread hatred, conspiracy and false information to create chaos, while damaging the American democracy.

Today, the United States has a choice in how to respond to these attacks. While the present diplomatic, law enforcement, private sector, regulatory and intelligence community response should continue, they alone have not proved a completely sufficient counterstrategy. Furthermore, the U.S. response through 2018 did not address informing or educating the American people about the danger presented by strategic weapons of influence. Propaganda education, combined with transparency about the threat, should be added to the toolbox. Following formulas from the "whole of society" model, the people should be given cognitive skills to identify strategic weapons of influence. This defense strategy may help ensure that authentic content continues to flow in an open, creative, and mutually beneficial manner uncensored, while possibly preventing negative outcomes from future information warfare attacks.

For a democracy to function, the government must trust the electorate to make good decisions fortified by education. U.S. political leaders should be honest with the American public about what took place surrounding the 2016 election and the ongoing threat from hostile propaganda over social media. While this approach might not fully prevent a negative impact on civil society from influence operations, it could certainly create more resilience in targeted populations.

The U.S. Department of Education could provide financial resources along with moral encouragement for school districts across the United States to implement

curriculums that teach critical thinking, especially in regards to propaganda, and mass media.

Another possibility would be to set up a public service campaign through the DHS to warn society of the dangers of hostile propaganda. This effort could be modeled on the “See Something, Say Something,” campaign used to engage U.S. residents around terrorism related threats. While raising awareness could also provoke some false reporting, the overall civic engagement in identifying influence operations, especially on social media, could further increase the public’s understanding of the legitimacy of the threat.

Additionally, the DHS, in a collaborative effort with other members of the U.S. intelligence community, should set up a public alert system for when an active foreign influence operation is targeting U.S. populations. This system could be modeled on the terror alert system implemented after the September 11 attacks.

Efforts are presently taking place in the private sector and through NGOs to monitor and alert around active influence operations on the internet. The Alliance for Securing Democracy, with its Russian disinformation bot tracking website Hamilton 68 states, “We are not telling you what to think, but we believe you should know when someone is trying to manipulate you. What you do with that information is up to you.”¹⁷⁸ While background and analysis on a propaganda bot tracking program out of Robhat Labs focused on Twitter, the Robhats Labs project uses algorithms to track political propaganda bots and a classifier to look at patterns.¹⁷⁹ An academic effort titled *The Computational Propaganda Project*, out of Oxford University in England states its aim is to, “investigates the interaction of algorithms, automation and politics. This work includes analysis of how tools like social media bots are used to manipulate public opinion by amplifying or repressing political content, disinformation, hate speech, and junk news.”¹⁸⁰

¹⁷⁸ Rosenberg and Berger, “Hamilton 68.”

¹⁷⁹ Robhat Labs, “An Analysis of Propaganda Bots on Twitter.”

¹⁸⁰ Oxford University, “The Computational Propaganda Project.”

Regardless of how effective NGO programs are, a full endorsement of the monitoring and alert concept, with the stamp of governmental legitimacy, can greatly increase civil society's awareness of this evolving threat. The DHS can also follow the Swedish model by producing educational material to help all levels of society understand the threat from influence operations. This increased awareness through education supported by real-time public alerts posted by the DHS can further elevate the public's ability to resist manipulation and thus create a more resilient society.

E. NO TIME FOR COMPLACENCE

The evolution of media technology will continue at a rapid pace. As a result, policy makers should not assume what works today for monitoring and mitigation of social media-based influence operations—whether it is by the private sector or by government—will work tomorrow. The strategy to countering strategic weapons of influence must be comprehensive and adaptable. It should include elements of today's response like diplomatic sanctions, economic sanctions, criminal prosecution, private sector self-regulation, and the ongoing efforts of NGOs as well as the free press to track the threat. Nevertheless, the additional elements not yet present in the U.S. counter strategy should be added. These elements include engaging civil society and teaching people to think critically about information. Americans should be provided information about the importance of questioning sources, being aware of emotional hooks, and pausing before forwarding, re-tweeting, or posting a piece of content on social media. Combined with a civic education on propaganda, the government should openly provide alerts when a largescale attack is identified. Simply falling back on the private sector regulation and non-governmental monitoring is not enough. A DHS warning system can provide credibility to the threat, while potentially increasing faith in government institutions and the democratic processes that supports them.

These counter strategies are proposed with an understanding for the likely malleability of delivery medium for future active measures campaigns. They transcend rapidly evolving technology and inevitable changes in the media environment. They offer an opportunity not just to blunt the impact of present strategic weapons of influence, but

also to strengthen fundamentally the integrity of the U.S. democracy, on which this nation's economic vibrancy and global leadership are built. See Figure 58.

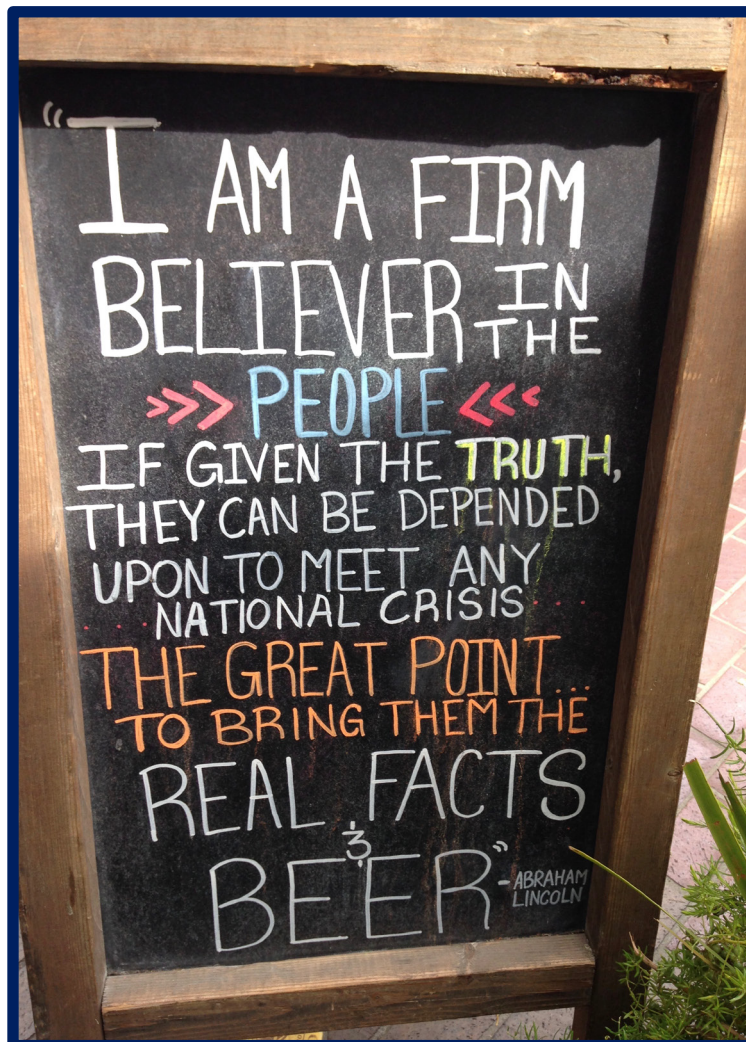


Figure 58. Sign Posted Out Front of the Alvarado Street Brewery, Monterey CA, 2018. Attribution to Abraham Lincoln Has Not Been Verified.

LIST OF REFERENCES

- Albright, Jonathan. "Trolls on Twitter: How Mainstream and Local News Outlets Were Used to Drive a Polarized News Agenda." Harvard University, February 15, 2018. <https://medium.com/berkman-klein-center/trolls-on-twitter-how-mainstream-and-local-news-outlets-were-used-to-drive-a-polarized-news-agenda-e8b514e4a37a>.
- Allcott, Hunt, Luca Braghieri, Sarah Eichmeyer, and Matthew Gentzkow. *The Welfare Effects of Social Media*. Palo Alto, CA: Stanford University, 2019. <http://web.stanford.edu/~gentzkow/research/facebook.pdf>.
- BBC. "Trump Worries NATO with 'Obsolete' Comment." January 16, 2017. <https://www.bbc.com/news/world-us-canada-38635181>.
- Bertrand, Natasha. "It Looks like Russia Hired Internet Trolls to Pose as Pro-Trump Americans." *Business Insider*, July 27, 2016. <http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7>.
- Bradshaw, Samantha, and Philip Howard. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Oxford: Oxford University, 2018. <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf>.
- Byers, Dylan. "Facebook Estimates 126 Million People Were Served Content from Russia-Linked Pages." CNN, October 31, 2017. <https://money.cnn.com/2017/10/30/media/russia-facebook-126-million-users/index.html?iid=EL>.
- Chen, Adrian. "The Agency." *New York Times Magazine*, June 2, 2015. <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>.
- Chivvis, Christopher S. "Hybrid War: Russian Contemporary Political Warfare." *Bulletin of the Atomic Scientists* 73, no. 5 (August 21, 2017): 316–321. <https://doi.org/10.1080/00963402.2017.1362903>.
- Christopher, Paul, and Miriam Matthews. *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. Santa Monica, CA: RAND, 2016. <https://www.rand.org/pubs/perspectives/PE198.html>.
- Committee on Foreign Relations. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*. Washington, DC: United States Senate, 2018.

- Conley, Heather, James Mina, Ruslan Stefanov, and Marin Vladimirov. *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe*. Lanham, MD: Rowman and Littlefield, 2016.
- Department of Justice. “Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election.” July 13, 2018. <https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>.
- Department of Treasury. “Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks.” March 15, 2018. <https://home.treasury.gov/news/press-releases/sm0312>.
- Digital Forensic Research Lab. “Logical Fallacies Fuel Kremlin Disinfo: How the Kremlin and its Disinformation Networks Use Logical Fallacies to Dismiss, Dismay, Distract and Distort.” April 22, 2018. <https://medium.com/dfrlab/logical-fallacies-fuel-kremlin-disinfo-e4185bb455e6>.
- Dimock, Michael. “Our Expanded Focus on Trust, Facts and the State of Democracy.” Pew Research Center, April 26, 2018. <http://www.pewresearch.org/2018/04/26/our-expanded-focus-on-trust-facts-and-the-state-of-democracy/>.
- Economist, The*. “Putin’s Russia: Repression Ahead.” 407, no. 8838 (June 1, 2013). <https://www.economist.com/europe/2013/06/01/repression-ahead>.
- Frenkel, Sheera, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg, and Jack Nicas. “Delay, Deny and Deflect: How Facebook’s Leaders Fought through Crisis.” *New York Times*, November 14, 2018. <https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html>.
- Frier, Sarah. “Facebook Says it Will Double Safety and Security Staff to 20,000.” *Bloomberg News*, October 31, 2017. <https://www.bloomberg.com/news/articles/2017-10-31/facebook-says-it-will-double-safety-and-security-staff-to-20-000>.
- Gallacher, John. *Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns against US Military Personnel and Veterans*. Oxford: Oxford University, 2017. <http://comprop.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/10/Junk-News-on-Military-Affairs-and-National-Security-1.pdf>.
- Gallagher, Erin. “Fighting Disinformation on Social Media.” Medium, October 9, 2018. https://medium.com/@erin_gallagher/best-practices-on-social-media-for-mid-term-elections-c821386d4ec0.

- Gingrich, Newt. "The Clinton Started the so-called Russian Collusion Scandal and May be Destroyed by It." Fox News, October 27, 2017. <https://www.foxnews.com/opinion/newt-gingrich-the-clintons-started-the-so-called-russian-collusion-scandal-and-may-be-destroyed-by-it>.
- Harbath, Katie, and Samidh Chakrabarti. "Expanding Our Efforts to Protect Elections in 2019." Facebook Newsroom, January 28, 2019. <https://newsroom.fb.com/news/2019/01/elections-2019/>.
- Holan, Angie Drobnić. "2017 Lie of the Year: Russian Election Interference a Made-Up Story." Politifact, December 12, 2017. <https://www.politifact.com/truth-o-meter/article/2017/dec/12/2017-lie-year-russian-election-interference-made-s/>.
- Howard, Philip, Dimitra Liotsiou, John Kelly, and Camille François. *The IRA, Social Media and Political Polarization in the United States, 2012–2018*. Oxford: Oxford University, 2018. <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf>.
- Huxley, Aldous. *Brave New World*. New York: Bantam Books, 1958.
- Klimburg, Alexander. *The Darkening Web: The War for Cyberspace*. New York: Penguin, 2017.
- Korta, Samantha. "Fake News Conspiracy Theories and Lies: An Information Laundering Model for Homeland Security." Master's thesis, Naval Postgraduate School, 2018.
- Kragh, Martin, and Sebastian Åsberg. "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case." *Journal of Strategic Studies* 40, no. 6 (2017): 773–816. doi: 10.1080/01402390.2016.1273830.
- McGeehan, Timothy. *Countering Russian Disinformation*. Carlisle, PA: Army War College, 2018. https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf.
- Ministry of Defence of the Russian Federation. *Russian Federation Armed Forces' Information Space Activities Concept*. Moscow: Ministry of Defence of the Russian Federation, 2011. <https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle>.
- Morgan, Jonathan, and Kris Shaffer. "Sockpuppets, Secessionists, and Breitbart, How Russia May Have Orchestrated a Massive Social Media Influence Campaign." Data for Democracy, March 31, 2017. <https://medium.com/data-for-democracy/sockpuppets-secessionists-and-breitbart-7171b1134cd5>.

- Nakashima, Ryan, and Barbara Ortutay. "AP Exclusive: Russia Twitter Trolls Deflected Trump Bad News." *Associated Press*, November 9, 2017. <https://apnews.com/fc9ab2b0bbc34f11bc10714100318ae1>.
- National Cybersecurity and Communications Integration Center. *Grizzly Steppe Russian Malicious Cyber Activity*. JAR-16-20296. Washington, DC: Department of Homeland Security/Federal Bureau of Investigation, 2016. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.
- Nimmo, Ben, Csongor Bajnoczki, Donara Barojan, and Kanishk Karan. "#TrollTracker: Facebook's Midterm Takedown, Analyzing the Accounts Attributed to Russia's Internet Research Agency." Digital Forensic Research Lab, November 13, 2018. <https://medium.com/dfrlab/trolltracker-facebooks-midterm-takedown-f3451ee5dc2>.
- Office of Strategic Communications. *Remarks as Prepared for Delivery by The Honorable Dan Coats, Director of National Intelligence Annual Threat Assessment Opening Statement, Tuesday, January 29, 2019*. Washington, DC: Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-01-29-ATA-Opening-Statement_Final.pdf.
- Office of the Director of National Intelligence. *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Washington, DC: National Intelligence Council, 2017. https://permanent.access.gpo.gov/gpo76345/ICA_2017_01.pdf.
- Orwell, George. *1984: A Novel*. New York: Signet Classic, 1977.
- Owen, Laura Hazard. "Facebook Probably Didn't Want to be Denying it Paid People to Create Fake News this Week, But Here We Are." NiemanLab, November 16, 2018. <http://www.niemanlab.org/2018/11/facebook-probably-didnt-want-to-be-denying-it-paid-people-to-create-fake-news-this-week-but-here-we-are/>.
- Oxford University. "The Computational Propaganda Project: Algorithms, Automation and Digital Politics." Last modified July 20, 2018. <http://comprop.oii.ox.ac.uk>.
- Palagi, Jamie. *Wrestling the Bear: The Rise of Russian Hybrid Warfare*. Norfolk, VA: Joint Forces Staff College Joint Advanced Warfighting School, 2015.
- Pariser, Eli. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. New York: Penguin Books, 2011.
- Pew Research Center. "Public Trust in Government: 1958–2017." December 14, 2017. <http://www.people-press.org/2017/05/03/public-trust-in-government-1958-2017/>.

- Robertson, Jordan, Michael Riley, and Andrew Willis. “Como hackear una eleccion.” *Bloomberg*, March 31, 2016. <https://www.bloomberg.com/features/2016-como-manipular-una-eleccion/>.
- Robhat Labs. “An Analysis of Propaganda Bots on Twitter.” October 30, 2017. <https://medium.com/@robhat/an-analysis-of-propaganda-bots-on-twitter-7b7ec57256ae>.
- Roemer, Timothy, and Zachary Wamp. “This Is the Best First Step to Stop Russian Meddling in Our Politics.” *The Hill*, October 26, 2017. <http://thehill.com/opinion/national-security/357238-this-is-the-best-first-step-to-stop-russian-meddling-in-our>.
- Rosenberg, Laura, and J. M. Berger. “Hamilton 68: A New Tool to Track Russian Disinformation on Twitter.” Alliance for Security Democracy, August 2, 2017. <https://securingdemocracy.gmfus.org/hamilton-68-a-new-tool-to-track-russian-disinformation-on-twitter/>.
- Sanger, David. “Obama Strikes Back at Russia for Election Hacking.” *New York Times*, December 29, 2016. <https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html>.
- Schafer, Bret. “A View from the Digital Trenches—Lessons from Year One of Hamilton 68.” Alliance for Security Democracy, November 21, 2018. <https://securingdemocracy.gmfus.org/a-view-from-the-digital-trenches-lessons-from-year-one-of-hamilton-68/>.
- Senate Select Committee on Intelligence. *Disinformation a Primer in Russian Active Measures and Influence Campaigns*. Washington, DC: Senate Select Committee on Intelligence, 2017. <https://www.gpo.gov/fdsys/pkg/CHRG-115shrg25362/pdf/CHRG-115shrg25362.pdf>.
- . *The Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent U.S. Elections*. Washington, DC: Senate Select Committee on Intelligence, 2018. https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf.
- Stahl, Lesley. “RT’s Editor-In-Chief on Election Meddling, Being Labeled Russian Propaganda.” CBS, January 7, 2017. <https://www.cbsnews.com/news/rt-editor-in-chief-on-election-meddling-russian-propaganda-label/>.
- Swedish Civil Contingencies Agency. *Important Information for the Population of Sweden: If Crisis or War Comes*. Karlstad: Swedish Civil Contingencies Agency, 2018.
- Tableau Public. “Troll Tweet Volume vs Date (ALL 36.5k Tweets).” 2016. https://public.tableau.com/shared/SNHTMKBRR?:display_count=yes&:showVizHome=no.

- Thomsen, Jaqueline. "US Cyber Operation Blocked Internet for Russian Troll Farm on Election Day 2018." *The Hill*, February 26, 2019. <https://thehill.com/policy/cyber-security/431614-us-cyber-operation-blocked-internet-for-russian-troll-farm-on-election>.
- Timberg, Craig, and Elizabeth Dwoskin. "Twitter is Sweeping out Fake Accounts like Never before: Putting User Growth at Risk." *Washington Post*, July 6, 2018. https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?utm_term=.d1ef26563774.
- U.S. Congress, House. Honest Ads Act. H. Res. 4077. 115th Cong., 1st sess., 2017–2018. <https://www.congress.gov/bill/115th-congress/house-bill/4077/text>.
- . *Report on Russian Active Measures*. Washington, DC: House Permanent Select Committee on Intelligence, 2018. <https://permanent.access.gpo.gov/gpo91495/HRPT-115-1.pdf>.
- U.S. Congress. Senate. *Russian Intervention in European Elections: United States Senate Select Committee on Intelligence*. 115th Cong., 1st sess., June 28, 2017.
- . *Testimony on Russian Interference in European Elections Senate Select Committee on Intelligence Ambassador (ret.) Nicholas Burns June 28, 2017*. 115th Cong., 1st sess., June 28, 2017. <https://www.intelligence.senate.gov/sites/default/files/documents/sfr-nburns-062817b.pdf>.
- United States House Committee on Energy and Commerce. *Testimony of Jack Dorsey Chief Executive of Twitter*. Washington, DC: U.S. House of Representatives, 2018. <https://docs.house.gov/meetings/IF/IF00/20180905/108642/HHRG-115-IF00-Wstate-DorseyJ-20180905.pdf>.
- UsHadrns. "This Space Is a Repository for Content from the Russian Social Media Account 'AfroKingdom_'" October 29, 2017. <https://medium.com/@ushadrns/this-space-is-a-repository-for-content-from-the-russian-twitter-account-afrokingdom-1ec195324086>.
- . "This Space Is a Repository for Content from the Russian Social Media Account 'AmericaFirst_'" March 17, 2018. <https://medium.com/@ushadrns/this-space-is-a-repository-for-content-from-the-russian-social-media-account-americafirst-a4081efeb761>.
- . "This Space Is a Repository for Content from the Russian Social Media Account 'Angry Eagle'" October 18, 2017. <https://medium.com/@ushadrns/this-space-is-a-repository-for-content-from-the-russian-social-media-group-angry-eagle-84d85140e71>.

- . “This Space Is a Repository for Content from the Russian Social Media Account ‘_Anonymous_news_.’” October 29, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-twitter-account-anonymous-news-fc3fb9e1bcea>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Army of Jesus’.” October 18, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-army-of-jesus-553c6aa74fea>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Being Patriotic’.” October 12, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-ads-from-the-russian-social-media-group-being-patriotic-4e823cad0a02>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Born Liberal’.” October 20, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-born-liberal-c55ae301335c>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Feminism_Tag’.” October 22, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-feminism-tag-24b2cf5a3525>.
- . “This Is Space Is a Repository for Content from the Russian Twitter Account ‘Jenna_Abrams’.” February 1, 2018. <https://medium.com/@ushadrons/this-is-space-is-a-repository-for-content-from-the-russian-twitter-account-jenna-abrams-c1570b468b86>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘MericanFury’.” October 25, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-mericanfury-7066546c96b>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Muslim_Voice’.” October 23, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-muslim-voice-b22bf2bc1c57>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Pamela_Moore13’.” October 27, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-pamela-moore13-a53525a1bc38>.

- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Rainbow_Nation_US’.” October 22, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-rainbow-nation-us-cc30ba458951>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Secured Borders’.” October 12, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-ads-from-the-russian-social-media-group-secured-borders-a62acfb7726>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘South United’.” October 17, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-south-united-35bcdeaa6f29>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Stop All Invaders’.” October 17, 2017. <https://medium.com/@ushadrons/stop-the-invasion-f8c93d774f97>.
- . “This Space Is a Repository for Content from the Russian Twitter Account ‘Ten_GOP’.” October 19, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-ten-gop-ed7e6cf6d30>.
- . “This Space Is a Repository for Content from the Russian Twitter Account ‘USA_Gunslinger’.” October 30, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-twitter-account-usa-gunslinger-538485a9224f>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘veterans_us’.” January 30, 2018. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-account-veterans-us-8c1beb0aa607>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Watch.the.Police’.” October 25, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-twitter-account-watch-the-police-e894e0269670>.
- . “This Space Is a Repository for Content from the Russian Social Media Account ‘Woke Blacks’.” October 19, 2017. <https://medium.com/@ushadrons/this-space-is-a-repository-for-content-from-the-russian-social-media-group-woke-blacks-d42b989ddd7f>.
- Vosoughi, Sorous, Deb Roy, and Sinan Aral. “The Spread of True and False News Online,” *Science* 359, no. 6380 (March 9, 2018): 1146–1151. <http://science.sciencemag.org/content/359/6380/1146>.

———. *The Spread of True and False News Online*. Cambridge, MA: MIT Initiative on the Digital Economy, 2017. <http://ide.mit.edu/sites/default/files/publications/2017%20IDE%20Research%20Brief%20False%20News.pdf>.

Wang, Selina. “California Would Require Twitter, Facebook to Disclose Bots.” *Bloomberg*, April 3, 2018. <https://www.bloomberg.com/news/articles/2018-04-03/california-would-require-twitter-facebook-to-disclose-bots>.

Wardle, Claire. “Fake News: It’s Complicated.” *First Draft*, February 16, 2017. <https://firstdraftnews.org/fake-news-complicated/>.

Zuckerberg, Mark. “Mark Zuckerberg.” Facebook, April 6, 2018. <https://www.facebook.com/zuck/posts/10104784125525891>.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California